

AN EXPLICIT RECIPROCITY LAW ARISING FROM SUPERSPECIAL ABELIAN VARIETIES AND TRACE FORMULAS

CHIA-FU YU

ABSTRACT. We develop a method for describing the Galois action on the superspecial locus in the mod p of the Siegel moduli space. Using this explicit description, we deduce and extend the results of Ibukiyama and Katsura that relate \mathbb{F}_{p^2} -rational points, closed points and \mathbb{F}_p -rational points in the superspecial locus in the geometric side, and the class number, type number and the trace of a Hecke operator of Atkin-Lehner type on a quaternion Hermitian form in the arithmetic side. We also calculate the traces of these Hecke operators using the Selberg trace formula.

1. INTRODUCTION

Throughout this paper p denotes a rational prime number. An abelian variety A over a field of characteristic p is said to be *superspecial* if it is isomorphic to a product of supersingular elliptic curves over an algebraic closure of the ground field. It is known that every supersingular elliptic curve E over any algebraically closed field k has a model defined over \mathbb{F}_{p^2} (see Deuring [2]); this means that there is an elliptic curve E' over \mathbb{F}_{p^2} and there is an isomorphism $E \simeq E' \otimes_{\mathbb{F}_{p^2}} k$ over k ; the elliptic curve E' is called a model of (the isomorphism class of) E over \mathbb{F}_{p^2} . For any $g > 1$, there is only one isomorphism class of g -dimensional superspecial abelian varieties over k (This fact is due to Shioda, Deligne and Ogus). Particularly every superspecial abelian variety of dimension greater than one over k has a model defined over \mathbb{F}_p . In [10] Ibukiyama and Katsura studied the field of definition of superspecial *polarized* abelian varieties. They showed that every superspecial principally polarized abelian variety over $\overline{\mathbb{F}}_p$ has a model defined over \mathbb{F}_{p^2} . They also expressed the number of those which have a model defined over \mathbb{F}_p in terms of the class number and the type number of the quaternion unitary algebraic group in question. See below for more details.

Let $\Lambda_g = \Lambda_g(\overline{\mathbb{F}}_p)$ denote the set of isomorphism classes of g -dimensional superspecial principally polarized abelian varieties over $\overline{\mathbb{F}}_p$. The goal of this paper is to develop a method for describing the action of the Galois group $\mathcal{G} := \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ on this finite set. We call this a reciprocity law because a reciprocity law, in a general sense, may be regarded as a description of a Galois group acting on a class space of adelic points in terms of Hecke translations. For CM fields, the Shimura-Taniyama reciprocity law tells us how the Galois group of the related reflex field acts on the spaces of CM abelian varieties explicitly; this is known as the main theorem of

Date: October 4, 2012.

2000 Mathematics Subject Classification. 14K10, 11E41, 11G18.

Key words and phrases. Superspecial abelian varieties, explicit reciprocity law, class number.

complex multiplication [29]. For the field of rational numbers, the action of the Galois group $G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the group of torsions points of the multiplicative group G_m over \mathbb{Q} gives rise to the cyclotomic character $\omega : G_{\mathbb{Q}} \rightarrow \hat{\mathbb{Z}}^{\times}$, which factors through an isomorphism $\omega : G_{\mathbb{Q}}^{\text{ab}} \simeq \hat{\mathbb{Z}}^{\times}$. By the isomorphism $\mathbb{R}_{>0}\mathbb{Q}^{\times} \backslash \mathbb{A}_{\mathbb{Q}}^{\times} \simeq \hat{\mathbb{Z}}^{\times}$ and inverting the cyclotomic character, we get a map $\text{rec}_{\mathbb{Q}} : \mathbb{Q}^{\times} \backslash \mathbb{A}_{\mathbb{Q}}^{\times} \rightarrow G_{\mathbb{Q}}^{\text{ab}}$, which is the Artin reciprocity map. The Artin reciprocity map classifies all abelian extensions of \mathbb{Q} and gives the explicit description of its maximal abelian extension, known as the Kronecker-Weber theorem (cf. [18, Part II]).

Let (A_0, λ_0) be a superspecial principally polarized abelian variety over \mathbb{F}_p , considered as the base point in Λ_g . To (A_0, λ_0) we associate two group schemes $G_1 \subset G$ over $\text{Spec } \mathbb{Z}$ as follows. For any commutative ring R , the groups of their R -valued points are defined as

$$G(R) := \{x \in (\text{End}_{\overline{\mathbb{F}}_p}(A_0) \otimes R)^{\times} \mid x'x \in R^{\times}\},$$

$$G_1(R) := \{x \in (\text{End}_{\overline{\mathbb{F}}_p}(A_0) \otimes R)^{\times} \mid x'x = 1\},$$

where the map $x \mapsto x'$ is the Rosati involution induced by the polarization λ_0 . For convenience, we often also write G_1 and G for their generic fibers $G_{1,\mathbb{Q}}$ and $G_{\mathbb{Q}}$, respectively. As a well-known fact (cf. [11], [4], [33, Theorem 10.5], or [37, Theorem 2.2]), there is a natural parametrization of Λ_g by the following double coset spaces

$$(1.1) \quad \mathbf{d} : G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / G(\hat{\mathbb{Z}}) = G_1(\mathbb{Q}) \backslash G_1(\mathbb{A}_f) / G_1(\hat{\mathbb{Z}}) \simeq \Lambda_g$$

in which the base point (A_0, λ_0) corresponds to the identity class [1], where $\hat{\mathbb{Z}}$ is the profinite completion of \mathbb{Z} and $\mathbb{A}_f = \hat{\mathbb{Z}} \otimes \mathbb{Q}$ is the finite adele ring of \mathbb{Q} . As the abelian variety A_0 is defined over \mathbb{F}_p , the Galois group \mathcal{G} acts naturally on the finite adelic group $G(\mathbb{A}_f)$. On the other hand, the group \mathcal{G} acts on the set $\mathcal{A}_g(\overline{\mathbb{F}}_p)$ of $\overline{\mathbb{F}}_p$ -points, where \mathcal{A}_g denotes the moduli space of g -dimensional principally polarized abelian varieties. It is easy to show that the superspecial locus Λ_g is invariant under this action (Corollary 4.2). Let $\sigma_p : x \mapsto x^p, x \in \overline{\mathbb{F}}_p$, be the (arithmetic) Frobenius automorphism in \mathcal{G} . We prove the following result.

Theorem 1.1.

(1) *The action of \mathcal{G} on $G(\mathbb{A}_f)$ is given by*

$$(1.2) \quad \sigma_p(x)_{\ell} = (\pi_0 x_{\ell} \pi_0^{-1})_{\ell}, \quad (x)_{\ell} \in G(\mathbb{A}_f),$$

where $\pi_0 \in G(\mathbb{Q})$ is the relative Frobenius morphism on A_0 over \mathbb{F}_p .

(2) *The natural map $\tilde{\mathbf{d}} : G(\mathbb{A}_f) \rightarrow \Lambda_g$ induced by (1.1) is \mathcal{G} -equivariant.*

We now explain the main results of Ibukiyama and Katsura in [10]. We can select the base point (A_0, λ_0) over \mathbb{F}_p so that the relative Frobenius endomorphism $\pi_0 \in \text{End}(A_0)$ satisfying $\pi_0^2 = -p$. The existence of (A_0, λ_0) is known due to Deuring (cf. [10]); this also follows from the Honda-Tate theory [30]. Put $U := G(\hat{\mathbb{Z}})$ and $U(\pi_0) := U\pi_0 = \pi_0 U$.

Theorem 1.2. ([10, Theorem 1])

(1) *Every member $(A, \lambda) \in \Lambda_g$ has a model defined over \mathbb{F}_{p^2} .*

- (2) Let (A, λ) be a member in Λ_g and let $[x] \in G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / U$ be the class corresponding to the isomorphism class $[(A, \lambda)]$. Then (A, λ) has a model defined over \mathbb{F}_p if and only if

$$(1.3) \quad G(\mathbb{Q}) \cap xU(\pi_0)x^{-1} \neq \emptyset.$$

The second part of work of Ibukiyama and Katsura concerns the trace of a Hecke operator of Atkin-Lehner type on the space of automorphic forms on the group G . Denote by $M_0(U)$ the vector space of all functions $f : G(\mathbb{A}_f) \rightarrow \mathbb{C}$ on $G(\mathbb{A}_f)$ that satisfy $f(axu) = f(x)$ for all $a \in G(\mathbb{Q})$ and $u \in U$. Let $\mathcal{H}(G, U)$ denote the convolution algebra of bi- U -invariant functions h on $G(\mathbb{A}_f)$ with compact support, called the Hecke algebra. The Hecke algebra $\mathcal{H}(G, U)$ acts naturally on the space $M_0(U)$ by the following rule:

$$(1.4) \quad h * f(x) = \int_{G(\mathbb{A}_f)} h(y)f(xy)dy, \quad \text{for } h \in \mathcal{H}(G, U), \quad f \in M_0(U),$$

where the Haar measure on $G(\mathbb{A}_f)$ is normalized with volume one on U . Explicitly, if we write the double coset UyU , where y is an element in $G(\mathbb{A}_f)$, into $\coprod_{i=1}^n y_i U$ and let $\mathbf{1}_{UyU}$ denote the characteristic function of UyU , then one has

$$(1.5) \quad \mathbf{1}_{UyU} * f(x) = \sum_{i=1}^n f(xy_i).$$

Let $R(\pi_0)$ be the operator induced from the characteristic function of the double coset $U(\pi_0)$.

Let $\mathcal{T}(G)$ denote the set of $G(\mathbb{Q})$ -conjugacy classes of maximal orders in the central simple algebra $\text{End}^0(A_0 \otimes \overline{\mathbb{F}}_p) = \text{End}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes \mathbb{Q}$ which are $G(\mathbb{A}_f)$ -conjugate to the maximal order $\text{End}(A_0 \otimes \overline{\mathbb{F}}_p)$. We can write

$$\mathcal{T}(G) = G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / \mathfrak{N},$$

where \mathfrak{N} is the open subgroup of $G(\mathbb{A}_f)$ that normalizes the ring $\text{End}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes \hat{\mathbb{Z}}$. The cardinality T of $\mathcal{T}(G)$ is called the type number of the group G , following Hashimoto-Ibukiyama [9]. In the case $g = 1$, the group G is equal to the multiplicative group of the quaternion \mathbb{Q} -algebra $B_{p,\infty}$ ramified exactly at $\{\infty, p\}$, and this coincides with the usual definition of the type number, namely the number of conjugacy classes of maximal orders in $B_{p,\infty}$.

Theorem 1.3. ([10, Theorem 2])

- (1) The number of members (A, λ) in Λ_g that have a model defined over \mathbb{F}_p is equal to $\text{tr } R(\pi_0)$.
- (2) We have $\text{tr } R(\pi_0) = 2T - H$, where H is the class number of G (for the level group U).

Remark that the case $g = 1$ of Theorems 1.2 and 1.3 is due to Deuring, and the case $g > 1$ is proved in [10].

As the main application of Theorem 1.1, we give a somehow simpler proof of Theorem 1.2 and Theorem 1.3 (1). Theorem 1.1 allows us to prove directly a statement relating the field of moduli of members in Λ_g (instead of the minimal field of definition) to the condition (1.3) and to the trace of the operator $R(\pi_0)$; see Proposition 6.2. However, this does not effect much as for any polarized abelian

variety (A, λ) over $\overline{\mathbb{F}}_p$, the field of moduli always agrees with the minimal field of definition for (A, λ) ; see Proposition 6.3 and Corollary 6.4. We also include an exposition of the proof of Theorem 1.3 (2) but in the language of adèles. As a byproduct, we obtain the following result (Theorem 6.9); this is implicit in the proof of [10, Theorem 2]. According to Theorem 1.1, the action of the Galois group \mathcal{G} on Λ_g factors through the quotient group $\text{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$. Let Λ_g^0 denote the set of closed points of Λ_g , viewed as a finite scheme over \mathbb{F}_p .

Theorem 1.4. *The composition $\Lambda_g \simeq G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / U \xrightarrow{\text{pr}} \mathcal{T}(G)$, where pr is the natural projection, induces a bijection between the set of $\text{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ -orbits of Λ_g and the set $\mathcal{T}(G)$. In other words, there is a natural bijection between the set Λ_g^0 of closed points in Λ_g and the set $\mathcal{T}(G)$.*

In some sense we have the following equality in the “arithmetic side”

$$(1.6) \quad \text{tr } R(\pi_0) = 2T - H$$

and its mirror in the geometric side

$$(1.7) \quad |\Lambda_g(\mathbb{F}_p)| = 2|\Lambda_g^0| - |\Lambda_g|$$

where $\Lambda_g(\mathbb{F}_p) \subset \Lambda_g$ is the subset of \mathbb{F}_p -rational points. Moreover, this is the term-by-term equality; see Theorems 1.3 and 1.4.

The computation of the class number H is extremely difficult; see [9] for the case $g = 2$. However, if we add a prime-to- p level structure to the superspecial locus and form a cover $\Lambda_{g,1,N}$ of Λ_g , then one can compute the cardinality $|\Lambda_{g,1,N}|$ rather easily using the mass formula:

$$|\Lambda_{g,1,N}| = |\text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})| \frac{(-1)^{g(g+1)/2}}{2^g} \left\{ \prod_{k=1}^g \zeta(1-2k) \right\} \cdot \prod_{k=1}^g \{p^k + (-1)^k\}.$$

See Ekedahl [4, p.159] and Hashimoto-Ibukiyama [9, Proposition 9], also cf. [36, Section 3]. This leads us to examine whether the analogous statement for (1.6) and (1.7) can be extended to the objects with prime-to- p level structures and whether all the terms can be computed explicitly.

We first describe the Galois action on the superspecial locus with a (usual) prime-to- p level structure. Let N be a prime-to- p positive integer. Let $\mathcal{A}_{g,1,N}$ denote the moduli space over $\overline{\mathbb{F}}_p$ of g -dimensional principally polarized abelian varieties with a (full) symplectic level- N structure; see Section 7.4 for details. Let $\tilde{\mathcal{A}}_g^{(p)} := (\mathcal{A}_{g,1,N})_{p \nmid N}$ be the tower of Siegel modular varieties with prime-to- p level structures, and let $\tilde{\Lambda}_g \subset \tilde{\mathcal{A}}_g^{(p)}(\overline{\mathbb{F}}_p)$ be the superspecial locus, which is the tower of superspecial loci $\Lambda_{g,1,N} \subset \mathcal{A}_{g,1,N}$ for all prime-to- p positive integers N . Let $T^{(p)}(A_0) := \prod_{\ell \neq p} T_\ell(A_0)$ be the prime-to- p Tate module of A_0 ; it is equipped with an action of \mathcal{G} so that we have a Galois representation

$$\rho : \mathcal{G} \rightarrow G(\hat{\mathbb{Z}}^{(p)}) \subset G(\mathbb{A}_f^p),$$

where $\hat{\mathbb{Z}}^{(p)} := \prod_{\ell \neq p} \mathbb{Z}_\ell$ and $\mathbb{A}_f^p := \hat{\mathbb{Z}}^{(p)} \otimes \mathbb{Q}$ is the prime-to- p finite adèle ring of \mathbb{Q} . We fix a point $(A_0, \lambda_0, \tilde{\alpha}_0) \in \tilde{\Lambda}_g$ over (A_0, λ_0) , where $\tilde{\alpha}_0 : (\hat{\mathbb{Z}}^{(p)})^{2g} \simeq T^{(p)}(A_0)$ is a trivialization which preserves the pairings up to an element in $(\hat{\mathbb{Z}}^{(p)})^\times$. The trivialization $\tilde{\alpha}_0$ induces an isomorphism i_0

$$i_0 : G(\mathbb{A}_f^p) \simeq \text{GSp}_{2g}(\mathbb{A}_f^p)$$

and a Galois representation ρ_0 :

$$\rho_0 = i_0 \circ \rho : \mathcal{G} \rightarrow \mathrm{GSp}_{2g}(\mathbb{A}_f^p).$$

Let \mathcal{G} act on $\mathrm{GSp}_{2g}(\mathbb{A}_f^p)$ by the action ρ_0 :

$$(1.8) \quad \sigma \cdot x = \rho_0(\sigma)x, \quad \forall \sigma \in \mathcal{G}, x \in \mathrm{GSp}_{2g}(\mathbb{A}_f^p).$$

We prove

Theorem 1.5. *There is an isomorphism (depending on the choice of $\tilde{\alpha}_0$)*

$$\mathbf{b}_0^p : \tilde{\Lambda}_g \simeq i_0(G(\mathbb{Z}_{(p)})) \backslash \mathrm{GSp}_{2g}(\mathbb{A}_f^p)$$

which is compatible with the right $\mathrm{GSp}_{2g}(\mathbb{A}_f^p)$ -action and the (left) \mathcal{G} -action.

The action of the Galois group \mathcal{G} on the finite subset $\Lambda_{g,1,N}$ somehow contains a twist which comes from the trivialization between $A_0[N]$ and $(\mathbb{Z}/N\mathbb{Z})^{2g}$. This forces the subset $\Lambda_{g,1,N}(\mathbb{F}_p)$ of \mathbb{F}_p -rational points *empty* when N is large. As a result, there are no analogous results of Ibukiyama and Katsura for $\Lambda_{g,1,N}$ in the geometric side. However, the formulation of the arithmetic side extends well without any modification. To remedy this, we construct a new level- N structure for members in Λ_g using the base point (A_0, λ_0) . This yields a cover $\Lambda_{g,N}^*$ of Λ_g on which the Galois action becomes well-behaved. Getting around in this way, Theorems 1.2, 1.3 and 1.4 can be generalized without any difficulty from the present approach; see Theorem 7.5. The advantage of the present formulation of increasing levels makes it more accessible in computing the size of the set $\Lambda_{g,N}^*(\mathbb{F}_p)$ of \mathbb{F}_p -rational points, as well as the type number with level structure (the number T_N in Theorem 7.5 (5)), when N is large enough. Note that we had an explicit formula for the class number $|\Lambda_{g,1,N}|$ due to Ekedahl and others.

To continue, we make an initial study of the Selberg trace formula (cf. [6]) for the group G . What we need is to compute the trace of a certain Hecke operator $R(\pi)$ on a group G with compact quotient $G(\mathbb{Q}) \backslash G(\mathbb{A}_f)$. When the level group is small, we reduce the calculation of trace of the Hecke operator $R(\pi)$ concerned, to computing the size of a certain global set $\Delta_f(\pi)$, the volume of a fundamental domain for the centralizer G_π of π , and a standard orbital integral which is purely local in nature; see Section 9 for details, especially Theorem 9.4. We remark that the finite set $\Delta_f(\pi)$ has an interesting cohomological meaning (see Section 9.5) and one can calculate the volume of fundamental domains explicitly using the methods of G. Prasad [23] or of Shimura [28].

The method of the present paper works for more general Shimura varieties. One can apply it to describe the Galois action on the so called *minimal basic locus* in the mod p of a PEL-type Shimura variety in the following sense: The basic locus is the unique minimal Newton stratum; a basic polarized abelian variety (A, λ, ι) with an O_B -action (O_B an order that is maximal at p , i.e. $O_B \otimes \mathbb{Z}_p$ is a maximal order, in a semi-simple \mathbb{Q} -algebra B with a positive involution) is called minimal if $\mathrm{End}_{O_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is a maximal order. These are natural generalizations of superspecial abelian varieties. See [16] and [25] for precise definitions of these moduli spaces and basic abelian varieties. The existence of basic points is known due to many people in many cases (see [30], [34], [5], [20], [35], [31]). The existence of minimal basic points can be deduced using the result [38, Theorem 1.3]. The parametrization of the minimal basic locus by a double coset space (similar to

(1.1)) is also available; see [37, Theorems 2.2 and 4.6]. The remaining ingredient for describing the Galois action is provided in the present paper.

There have been a theory of modular forms mod p initiated by Serre [27] and more generally on algebraic modular forms developed by Gross [8]. Under the framework of Gross' theory, Ghitza proved the Jacquet-Langlands correspondence modulo p between modular forms on GSp_{2g} and algebraic modular forms on its compact inner form "twisted at p and ∞ ". He obtained this by restricting modular forms mod p to the Siegel superspecial locus, and used the meaning of modular forms as global sections of an automorphic bundle. See loc. cit. for more details. This beautiful result has been carried over very recently by Reduzzi [26] for the Shimura varieties attached to unitary groups $GU(r, s)$ associated to imaginary quadratic fields where the prime p is inert. Hopefully results in the present paper or strengthened ones could contribute to a construction of Galois representations attached to algebraic modular forms expected in Gross [8, Chapter IV].

The paper is organized as follows. Section 2 collects elementary properties of schemes transformed by Galois groups. Section 3 recalls Weil's theorems on the descent theory for varieties. These two sections are included only for the reader's convenience. In Section 4 we prove that the superspecial locus is stable under the Galois action. The analogous results for Newton strata and EO strata are also obtained. Proof of Theorem 1.1 is given in Section 5. In Section 6 we show that results of Ibukiyama-Katsura mentioned above are consequences of Theorem 1.1. In Section 7, we treat the situation with a prime-to- p level structure and generalize the results of Ibukiyama and Katsura to superspecial abelian varieties with level structures. The analogous results for the *non-principal genus* case are included in Section 8. We abstract the properties of computing $\mathrm{tr} R(\pi_0)$ and work on the trace formula in a slightly more general content. As a result, we reduce the calculation of trace of $R(\pi)$ to certain more manageable terms when the level group is small.

2. PRELIMINARIES

In this section we collect elementary properties about schemes transformed by Galois groups. This is only for the reader's convenience. The reader who has these basic concepts may skip this section.

2.1. Let $f : X \rightarrow S$ be a morphism of schemes, and let $\tau : T \rightarrow S$ be a base morphism. Write $X_T := X \times_S T$ for the fiber product, and hence we have the cartesian diagram

$$(2.1) \quad \begin{array}{ccc} X_T & \xrightarrow{\tau_X} & X \\ \downarrow f_T & & \downarrow f \\ T & \xrightarrow{\tau} & S \end{array}$$

Suppose that $X = \mathrm{Spec} R \rightarrow S = \mathrm{Spec} A$ is an affine scheme of finite type over A and $T = \mathrm{Spec} B$ is an affine scheme, where A , B and R are commutative rings, and the morphism $\tau : T = \mathrm{Spec} B \rightarrow \mathrm{Spec} A$ is induced by a ring homomorphism $\varphi : A \rightarrow B$. If we write $R = A[X_1, \dots, X_n]/(f_j)_j$, then $R \otimes_A B = B[X_1, \dots, X_n]/(F_j)_j$, where F_j is the polynomial over B obtained by applying the coefficients of f_j through the ring map φ . Therefore, we may think of X_T (for

general schemes $T \rightarrow S$ and general S -schemes $X \rightarrow S$) the scheme which is obtained by applying the coefficients of “defining equations” for X/S through the map $\mathcal{O}_S \rightarrow \mathcal{O}_T$.

Let T' be a T -scheme. One can regard T' as an S -scheme through the morphism $\tau : T \rightarrow S$. For any T' -valued point t' of X_T , the morphism τ_X induces a T' -valued point $\tau_X t'$ of X :

$$(2.2) \quad \tau_X : X_T(T') \longrightarrow X_S(T').$$

See the diagram:

$$\begin{array}{ccccc} & & \tau_X t' & & \\ & \nearrow & & \searrow & \\ T' & \xrightarrow{t'} & X_T & \xrightarrow{\tau_X} & X \\ & \searrow & \downarrow f_T & & \downarrow f \\ & & T & \xrightarrow{\tau} & S. \end{array}$$

The functorial property shows that the map (2.2) is a bijection. If $S = \operatorname{Spec} k$, $T = \operatorname{Spec} K$, and $T' = \operatorname{Spec} L$ are the spectra of fields $k \subset K \subset L$ and X is of finite type over k , then $X_K = X \otimes_k K$ is the “same variety” as X_k but allowing more functions with coefficients in K . It might be better to understand this “identification” by the bijection $X_K(L) \simeq X_k(L)$. We can make this “identification” more reasonable in the following sense. If we regard X as a functor F_X from the category of S -schemes to the category of sets, then X_T is simply the scheme which represents the functor F_X restricted to the category of T -schemes.

2.2. Let $f : X \rightarrow S$ and $\tau : T \rightarrow S$ be as above. We regard X as a contravariant functor. Therefore, any S -valued point s of $f : X \rightarrow S$ induces a T -valued point $s\tau$ of X over S :

$$(2.3) \quad X(S) \xrightarrow{\tau^*} X(T) = X_T(T).$$

By the functorial property of fiber products, this gives rise to a T -valued point of $f_T : X_T \rightarrow T$.

Suppose that $S = \operatorname{Spec} A$ is an affine scheme. For any element σ in $\operatorname{Aut}(A)$, the group of ring automorphisms of A , denote by

$$(2.4) \quad {}^\sigma X := X \times_{S, \sigma^*} S$$

the base change of X with respect to the morphism $\sigma^* : S \rightarrow S$ induced by σ . We write $\sigma_X^* : {}^\sigma X \rightarrow X$ for the induced isomorphism. Notice that as schemes, we have a natural morphism from ${}^\sigma X$ to X only. The naive Galois action on the *solutions* of X gives a mapping, through (2.3),

$$(2.5) \quad \sigma_* : X(A) \longrightarrow {}^\sigma X(A).$$

However, there is no natural morphism of schemes from X to ${}^\sigma X$ which induces the map σ_* in (2.5).

For any two elements $\sigma_1, \sigma_2 \in \text{Aut}(A)$, we have the following cartesian diagram:

$$(2.6) \quad \begin{array}{ccccc} \sigma_1(\sigma_2 X) & \xrightarrow{(\sigma_1^*)_{(\sigma_2 X)}} & \sigma_2 X & \xrightarrow{(\sigma_2^*)_X} & X \\ \downarrow \sigma_1(\sigma_2 f) & & \downarrow \sigma_2 f & & \downarrow f \\ S & \xrightarrow{\sigma_1^*} & S & \xrightarrow{\sigma_2^*} & S. \end{array}$$

It is easy to see that the following relations hold

$$(2.7) \quad \sigma_2^* \circ \sigma_1^* = (\sigma_1 \sigma_2)^*, \quad \sigma_1(\sigma_2 X) = \sigma_1 \sigma_2 X, \quad \text{and} \quad (\sigma_2^*)_X \circ (\sigma_1^*)_{(\sigma_2 X)} = (\sigma_1 \sigma_2)_X^*.$$

As for the mapping σ_* , we have the relation $\sigma_{1*} \sigma_{2*} = (\sigma_1 \sigma_2)_*$ for $\sigma_1, \sigma_2 \in \text{Aut}(A)$; see below:

$$(2.8) \quad X(A) \xrightarrow{\sigma_{2*}} \sigma_2 X(A) \xrightarrow{\sigma_{1*}} \sigma_1 \sigma_2 X(A).$$

We remark that the relations and properties above still hold if we replace the automorphism group $\text{Aut}(A)$ by the monoid $\text{End}(A)$ of ring endomorphisms of A .

It might be good to include basic properties of schemes transformed by the automorphism group $\text{Aut}(S)$ of the base scheme S as well, though they are exactly the same thing. Let $f : X \rightarrow S$ be an S -scheme. For $\tau \in \text{Aut}(S)$, denote by

$$(2.9) \quad X^\tau := X \times_{S, \tau} S$$

the base change of X with respect to the morphism $\tau : S \rightarrow S$. We write $\tau_X : X^\tau \rightarrow X$ for the induced isomorphism.

For $\tau_1, \tau_2 \in \text{Aut}(S)$, we have the following cartesian diagram:

$$(2.10) \quad \begin{array}{ccccc} (X^{\tau_1})^{\tau_2} & \xrightarrow{(\tau_2)_{(X^{\tau_1})}} & X^{\tau_1} & \xrightarrow{(\tau_1)_X} & X \\ \downarrow (f^{\tau_1})^{\tau_2} & & \downarrow f^{\tau_1} & & \downarrow f \\ S & \xrightarrow{\tau_2} & S & \xrightarrow{\tau_1} & S. \end{array}$$

It is easy to see that the relations hold

$$(2.11) \quad (X^{\tau_1})^{\tau_2} = X^{\tau_1 \tau_2}, \quad \text{and} \quad (\tau_1)_X \circ (\tau_2)_{(X^{\tau_1})} = (\tau_1 \tau_2)_X.$$

As mentioned before, the relations and properties above still hold if we replace the automorphism group $\text{Aut}(S)$ by the monoid $\text{End}(S)$ of endomorphisms of the scheme S .

2.3. Let $f_X : X \rightarrow S$ and $f_Y : Y \rightarrow S$ be two schemes over S . Let $\tau : T \rightarrow S$ be a morphism of schemes. If $f : X \rightarrow Y$ is a morphism of schemes over S , then we denote by $f^\tau : X_T \rightarrow Y_T$ the induced morphism of schemes over T . So we have the following cartesian diagram

$$(2.12) \quad \begin{array}{ccc} X_T & \xrightarrow{\tau_X} & X \\ \downarrow f^\tau & & \downarrow f \\ Y_T & \xrightarrow{\tau_Y} & Y. \end{array}$$

Let $\tau' : T' \rightarrow T$ be a T -scheme, and hence $\tau\tau' : T' \rightarrow S$ is an S -scheme. We have the following cartesian diagram

$$(2.13) \quad \begin{array}{ccccc} X_{T'} & \xrightarrow{\tau'_{X_T}} & X_T & \xrightarrow{\tau_X} & X \\ \downarrow (f^\tau)^{\tau'} & & \downarrow f^\tau & & \downarrow f \\ Y_{T'} & \xrightarrow{\tau'_{Y_T}} & Y_T & \xrightarrow{\tau_Y} & Y, \end{array}$$

and the relations

$$(2.14) \quad (f^\tau)^{\tau'} = f^{\tau\tau'}, \quad \tau_X \circ \tau'_{X_T} = (\tau\tau')_X, \quad \text{and} \quad \tau_Y \circ \tau'_{Y_T} = (\tau\tau')_Y.$$

Suppose that $S = \text{Spec } A$ and $T = \text{Spec } B$ are affine schemes, the morphism $\tau : \text{Spec } B \rightarrow \text{Spec } A$ is induced by a ring homomorphism $\varphi : A \rightarrow B$ of commutative rings, and $X = \text{Spec } R_X$ and $Y = \text{Spec } R_Y$ are affine schemes of finite type over S . Let $f : X \rightarrow Y$ be a morphism of schemes over S , and suppose that f is given by an A -homomorphism $\alpha : R_Y \rightarrow R_X$. If we write $R_Y = A[Y_1, \dots, Y_m]/(g_i)$, then α is given by a system of polynomial functions (in fact, they are elements in R_X) $\alpha_1, \dots, \alpha_m$ with coefficients in A . By definition, the morphism f^τ is induced by the B -homomorphism $\alpha_B : B \otimes_A R_Y \rightarrow B \otimes_A R_X$. We may regard α_B as a system of polynomial functions $\alpha_{1,B}, \dots, \alpha_{m,B}$ by applying their coefficients through the mapping $\varphi : A \rightarrow B$. In other word, the morphism $f^\tau : X_T \rightarrow Y_T$ is simply the one obtained by applying coefficients of the defining polynomial functions for f through the mapping $\mathcal{O}_S \rightarrow \mathcal{O}_T$. It follows from this description that we have the following commutative diagram (cf. (2.3)) of sets

$$(2.15) \quad \begin{array}{ccc} X(S) & \xrightarrow{\tau^*} & X_T(T) \\ \downarrow f & & \downarrow f^\tau \\ Y(S) & \xrightarrow{\tau^*} & Y_T(T) \end{array}$$

Notice that we do not have naturally a commutative diagram of schemes as follows

$$\begin{array}{ccc} X & \longrightarrow & X_T \\ \downarrow f & & \downarrow f^\tau \\ Y & \longrightarrow & Y_T. \end{array}$$

However, in some special situation we do have such an analogue; see (4.2).

2.4. Let $f_X : X \rightarrow S$ and $f_Y : Y \rightarrow S$ be two schemes over S , and let $\tau_0 : T \rightarrow S$ be an S -scheme. Let

$$M := \text{Hom}_T(X_T, Y_T), \quad \text{and} \quad H := \text{Aut}(T/S).$$

We describe the action of H on the set M . Write again $f_X : X_T \rightarrow T$ and $f_Y : Y_T \rightarrow T$ for the base change structure morphisms. For each element $\tau \in H$, we have the cartesian diagram

$$(2.16) \quad \begin{array}{ccc} X_T & \xrightarrow{\tau_X} & X_T \\ \downarrow f_X & & \downarrow f_X \\ T & \xrightarrow{\tau} & T. \end{array}$$

If $\tau_1, \tau_2 \in H$, then we have the following diagram (cf. (2.10))

$$(2.17) \quad \begin{array}{ccccc} X_T & \xrightarrow{(\tau_2)_X} & X_T & \xrightarrow{(\tau_1)_X} & X_T \\ \downarrow f_X & & \downarrow f_X & & \downarrow f_X \\ T & \xrightarrow{\tau_2} & T & \xrightarrow{\tau_1} & T, \end{array}$$

and the relations $(\tau_1)_X \circ (\tau_2)_X = (\tau_1 \tau_2)_X$.

For each element $\tau \in H$ and each morphism $f \in M$, the action of τ on f is defined to be f^τ (see Section 2.3):

$$(2.18) \quad \begin{array}{ccc} X_T & \xrightarrow{\tau_X} & X_T \\ \downarrow f^\tau & & \downarrow f \\ Y_T & \xrightarrow{\tau_Y} & Y_T. \end{array}$$

It is easy to see (cf. (2.4)) that $(f^{\tau_1})^{\tau_2} = f^{\tau_1 \tau_2}$, for $\tau_1, \tau_2 \in H$. That is, the group G acts on M from the right.

Suppose that $S = \text{Spec } A$ and $T = \text{Spec } B$ are affine. Let $H^* := \text{Aut}_A(B)$ be the group of A -automorphisms of B . For each element $\sigma \in H^*$ and $f \in M$, the action of σ on f is defined to be $\sigma(f) := {}^\sigma f$ (see (2.6)) in the cartesian diagram:

$$(2.19) \quad \begin{array}{ccc} X_T & \xrightarrow{\sigma_X^*} & X_T \\ \downarrow \sigma(f) & & \downarrow f \\ Y_T & \xrightarrow{\sigma_Y^*} & Y_T. \end{array}$$

It is easy to see (cf. (2.6)) that $\sigma_1(\sigma_2(f)) = (\sigma_1 \sigma_2)(f)$, for $\sigma_1, \sigma_2 \in H^*$. That is, the group $H^* = \text{Aut}_A(B)$ acts on the set $\text{Hom}_B(X \otimes_A B, Y \otimes_A B)$ from the left.

3. THE FIELD OF DEFINITION OF VARIETIES, FOLLOWING WEIL [32]

In this section we review the theory of the field of definition of varieties. We follow the well-known paper by Weil [32]. We fix a universal domain Ω , which is, by definition, an algebraically closed field that has infinite transcendence degree over its prime subfield. All fields considered in this section are subfields of Ω . By a variety over a field k we mean a scheme of finite type of k that is geometrically irreducible. Let k/k_0 be a field extension; we say a variety V over k is defined over k_0 if there is a variety V_0 over k_0 and there is an isomorphism $f : V_0 \otimes_{k_0} k \simeq V$ of varieties over k . In this case, the pair (V_0, f) is called a model of V over k_0 . In the classical language of algebraic geometry due to Weil [32], a generic point of a variety T over a field k is understood to be a geometric point $t \in T(\Omega)$ with the following property: suppose $U = \text{Spec } A \subset T$ is a k -open affine subvariety, where A is a finitely generated k -algebra, so that the geometric point t factors through $t : \text{Spec } \Omega \rightarrow U$, then the induced ring homomorphism $A \rightarrow \Omega$ is monomorphism. We call another generic point t' is *independent* of t if t' is a generic point of the variety $T \otimes_k k(t)$ over $k(t)$.

3.1. Finite separable field extensions. Let k be a finite separable extension of a field k_0 , and let V be a variety over k . Let \bar{k}_0 be the algebraic closure of k_0 , and let $\mathcal{J} := \text{Hom}_{k_0}(k, \bar{k}_0)$ be the set of field embeddings of k into \bar{k}_0 over k_0 . The Galois group $\mathcal{G}_{k_0} := \text{Gal}(\bar{k}_0/k_0)$ acts naturally on the finite set \mathcal{J} from the left: For $\sigma \in \mathcal{J}$ and $\omega \in \mathcal{G}_{k_0}$, set $\omega\sigma = \omega \circ \sigma$. For each element $\sigma \in \mathcal{J}$, we write ${}^\sigma V$ for the variety $V \otimes_{k, \sigma} \bar{k}_0$ over \bar{k}_0 . Suppose that there is a variety V_0 over k_0 and there is an isomorphism $f : V_0 \otimes_{k_0} k \simeq V$ of varieties over k . For each $\sigma \in \mathcal{J}$, we have an isomorphism ${}^\sigma f : {}^\sigma V_0 := V_0 \otimes_{k_0} \bar{k}_0 \xrightarrow{\sigma} {}^\sigma V$ over \bar{k}_0 . Then, for $\sigma, \tau \in \mathcal{J}$, we have an isomorphism

$$f_{\tau, \sigma} := {}^\tau f \circ ({}^\sigma f)^{-1} : {}^\sigma V \rightarrow {}^\tau V$$

of varieties over \bar{k}_0 . It is easy to check that the morphisms $f_{\tau, \sigma}$ satisfy the following conditions:

- (i) $f_{\tau, \rho} = f_{\tau, \sigma} \circ f_{\sigma, \rho}$ for all $\tau, \sigma, \rho \in \mathcal{J}$.
- (ii) $f_{\omega\tau, \omega\sigma} = \omega(f_{\tau, \sigma})$ for all $\tau, \sigma \in \mathcal{J}$ and $\omega \in \mathcal{G}_{k_0}$.

Conversely, Weil showed that these necessary conditions are also sufficient for V over k to have a model (V_0, f) over k_0 , provided that V is quasi-projective over k .

Theorem 3.1. (Weil [32, Theorem 3]) *Notations as above. Assume that V is quasi-projective over k , and that for each pair of elements $\tau, \sigma \in \mathcal{J}$, there is an isomorphism $f_{\tau, \sigma} : {}^\sigma V \rightarrow {}^\tau V$ such that the conditions (i) and (ii) are satisfied. Then there is a model (V_0, f) of V over k_0 , unique up to an isomorphism over k_0 , so that $f_{\tau, \sigma} = {}^\tau f \circ ({}^\sigma f)^{-1}$, for all $\tau, \sigma \in \mathcal{J}$.*

Moreover, if V is quasi-projective (resp. affine), then the variety V_0 is quasi-projective (resp. affine).

If the extension k/k_0 is Galois, letting $a_\sigma := f_{\sigma, 1} : V \rightarrow {}^\sigma V$, then the conditions (i) and (ii) are equivalent to the 1-cocycle condition $a_{\tau\sigma} = {}^\tau(a_\sigma) \circ a_\tau$ for all $\tau, \sigma \in \text{Gal}(k/k_0)$:

$$\begin{array}{ccccc} & & a_{\tau\sigma} & & \\ & \searrow & & \nearrow & \\ V & \xrightarrow{a_\tau} & {}^\tau V & \xrightarrow{{}^\tau(a_\sigma)} & {}^{\tau\sigma} V. \end{array}$$

3.2. Regular field extensions. Let now k denote the ground field. Let T be a variety over k , and let t be a generic point of T over k . Let V_t be a variety over $k(t)$. If t' is also a generic point of V over k , then we write $V_{t'}$ for the variety $V_t \otimes_{k(t), \sigma} k(t')$ over $k(t')$, where $\sigma : k(t) \rightarrow k(t')$ is the k -isomorphism that sends t to t' . If $f_t : V_t \rightarrow W_t$ is a morphism of varieties over $k(t)$, then we write $f_{t'}$ for the induced morphism from $V_{t'}$ to $W_{t'}$ over $k(t')$. If $f_{t', t} : V_{t', t} \rightarrow W_{t', t}$ is a morphism of varieties over $k(t, t')$ and t'' is another generic point of T over k , then we write $f_{t'', t'}$ for the induced morphism

$$V_{t', t} \otimes_{k(t, t'), \sigma} k(t', t'') \rightarrow W_{t', t} \otimes_{k(t, t'), \sigma} k(t', t'')$$

over $k(t', t'')$, where $\sigma : k(t, t') \simeq k(t', t'')$ is a k -isomorphism that sends (t, t') to (t', t'') .

Suppose that there are a variety V over k and an isomorphism $f_t : V \otimes_k k(t) \simeq V_t$ over $k(t)$. Then for any generic point t' over T over k , the morphism

$$f_{t', t} := f_{t'} \circ f_t^{-1} : V_t \rightarrow V_{t'}$$

is an isomorphism over $k(t, t')$. It is easy to check that the following property holds:

(i) We have $f_{t'',t} = f_{t'',t'} \circ f_{t',t}$, where t'' is a generic point of $T \otimes_k k(t, t')$ over $k(t, t')$.

Conversely, Weil showed that this necessary condition is also sufficient for the variety V_t over $k(t)$ to have a model (V, f) over k .

Theorem 3.2. (Weil [32, Theorem 6]) *Let T, t, V_t be as above, and let t' be a generic point of T over k independent of t . Suppose there is an isomorphism $f_{t',t} : V_t \simeq V_{t'}$ over $k(t, t')$ such that the condition (i) holds. Then there is a model (V, f_t) of V_t over k , unique up to an isomorphism over k , so that $f_{t',t} = f_{t'} \circ f_t^{-1}$.*

Note that the assumption that V_t is quasi-projective as in Theorem 3.1 is not required here.

3.3. As to whether the model obtained in Theorems 3.1 and 3.2 admits a projective or affine embedding, Weil showed the following theorem

Theorem 3.3. (Weil [32, Theorem 7]) *Let K be a finitely generated field extension of k , and let V be a variety over k . If $V \otimes_k K$ is quasi-projective (resp. quasi-affine) over K , then V is quasi-projective (resp. quasi-affine) over k provided (i) K is separable over k or (ii) V is normal.*

4. ABELIAN VARIETIES IN CHARACTERISTIC p

4.1. Let S be an \mathbb{F}_p -scheme, and let $f_X : X \rightarrow S$ be an S -scheme. Denote by $F_S : S \rightarrow S$ (resp. $F_X : X \rightarrow X$) the Frobenius morphism on S (resp. on X), which is obtained by raising to the p -th power on its functions. Denote by

$$X^{(p)} := X \times_{S, F_S} S$$

the base change of X with respect to the morphism F_S . Let $F_{X/S}$ be the relative Frobenius morphism of X over S , which is defined by the following diagram:

$$(4.1) \quad \begin{array}{ccccc} X & & \xrightarrow{F_X} & & X \\ & \searrow F_{X/S} & & & \uparrow \\ & & X^{(p)} & \xrightarrow{\quad} & X \\ & \searrow f & \downarrow f_X^{(p)} & & \downarrow f_X \\ & & S & \xrightarrow{F_S} & S \end{array}$$

Let $f_Y : Y \rightarrow S$ be an S -scheme, and let $f : X \rightarrow Y$ be a morphism of schemes over S . We write $f^{(p)}$ for the morphism $X^{(p)} \rightarrow Y^{(p)}$ induced by the base change morphism $F_S : S \rightarrow S$. Hence, we have the cartesian diagram and commutative diagram

$$(4.2) \quad \begin{array}{ccccc} X^{(p)} & \longrightarrow & X & & X \xrightarrow{F_{X/S}} X^{(p)} \\ \downarrow f^{(p)} & & \downarrow f & & \downarrow f \\ Y^{(p)} & \longrightarrow & Y & & Y \xrightarrow{F_{Y/S}} Y^{(p)} \end{array}$$

Notice that the later diagram is not necessarily cartesian. If we write $Frob_p$ for the Frobenius map $\mathcal{O}_S \rightarrow \mathcal{O}_S$ raising to the p -th power, then we also write $Frob_p(f)$ for $f^{(p)}$.

4.2. Let A be an abelian variety over a perfect field k of characteristic p . Let $M^*(A)$ be the classical contravariant Dieudonné module of A . Let $W(k)$ be the ring of Witt vectors over k , and let σ_p be the Frobenius map on $W(k)$. If K is a perfect field containing the field k , then we have

$$(4.3) \quad M^*(A \otimes_k K) = W(K) \otimes_{W(k)} M^*(A).$$

In particular, we have

$$(4.4) \quad M^*(A^{(p)}) = W(k) \otimes_{W(k), \sigma_p} M^*(A)$$

By definition, the Frobenius map F on $M^*(A)$ is given by the composition of the $(W(k)$ -linear) pull-back map

$$F_{X/k}^* : M^*(A^{(p)}) \rightarrow M^*(A)$$

and the σ_p -linear map

$$1 \otimes \text{id} : M^*(A) \rightarrow W(k) \otimes_{W(k), \sigma_p} M^*(A) = M^*(A^{(p)}).$$

Proposition 4.1. *Let X be a p -divisible group over an algebraically closed field k of characteristic p , and let σ be an automorphism of the field k .*

- (1) *The p -divisible groups X and ${}^\sigma X$ have the same Newton polygon.*
- (2) *The p -divisible groups X and ${}^\sigma X$ have the same Ekedahl-Oort type. That is, there is an isomorphism $X[p] \simeq {}^\sigma X[p]$ of finite group schemes over k , where $X[p]$ denotes the finite subgroup scheme of p -torsions of X .*
- (3) *If X is superspecial, then so ${}^\sigma X$ is.*

PROOF. (1) Let X_0 be a p -divisible group over \mathbb{F}_p which has the same Newton polygon as X does. Choose an isogeny $\varphi : X_0 \rightarrow X$ over k . Then we have

$$\begin{array}{ccccc} X & \xleftarrow{\varphi} & X_0 & = & {}^\sigma X_0 & \xrightarrow{{}^\sigma \varphi} & {}^\sigma X \\ & \searrow f & \downarrow f_0 = {}^\sigma f_0 & & \swarrow {}^\sigma f & & \\ & & \text{Spec } k & & & & \end{array}$$

This shows that there is an isogeny between the p -divisible groups X and ${}^\sigma X$.

(2) According to the classification of the truncated BT groups of level 1 (see [22]), there is a p -divisible group X_0 over \mathbb{F}_p such that an isomorphism $X[p] \simeq X_0[p]$ over k exists. Applying the automorphism σ on this isomorphism, we get an isomorphism ${}^\sigma X[p] \simeq {}^\sigma X_0[p] = X_0[p]$ over k . This proves (2).

(3) Since X is superspecial, we have $FM^*(X) = VM^*(X)$. This yields that $FM^*({}^\sigma X) = VM^*({}^\sigma X)$. Therefore, the p -divisible group ${}^\sigma X$ is superspecial. ■

Recall that \mathcal{A}_g denotes the moduli space of g -dimensional principally polarized abelian varieties, and that $\Lambda_g \subset \mathcal{A}_g(\overline{\mathbb{F}}_p)$ is the finite subset consisting of superspecial abelian varieties. For any abelian variety A over a field of characteristic p , we write $A(\ell) := A[\ell^\infty]$ for the associated ℓ -divisible group, and $T_\ell(A)$ for the Tate module module of A in the case $\ell \neq p$.

Corollary 4.2. *The action of the Galois group $\mathcal{G} := \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ on the set $\mathcal{A}_g(\overline{\mathbb{F}}_p)$ leaves the superspecial locus Λ_g invariant.*

4.3. Let A_0 be an abelian variety over \mathbb{F}_p . Let π_0 be the relative Frobenius morphism on A_0 over \mathbb{F}_p . Let σ_p be the arithmetic Frobenius element of the Galois group \mathcal{G} .

Proposition 4.3. *Notations as above.*

- (1) *For any endomorphism $f \in \text{End}_{\overline{\mathbb{F}}_p}(A_0 \otimes \overline{\mathbb{F}}_p)$ of $A_0 \otimes \overline{\mathbb{F}}_p$, we have the commutative diagram of abelian varieties over $\overline{\mathbb{F}}_p$*

$$(4.5) \quad \begin{array}{ccc} A_0 \otimes \overline{\mathbb{F}}_p & \xrightarrow{f} & A_0 \otimes \overline{\mathbb{F}}_p \\ \downarrow \pi_0 & & \downarrow \pi_0 \\ A_0 \otimes \overline{\mathbb{F}}_p & \xrightarrow{\sigma_p(f)} & A_0 \otimes \overline{\mathbb{F}}_p. \end{array}$$

- (2) *For any prime ℓ and any endomorphism f of the ℓ -divisible group $A_0(\ell) \otimes \overline{\mathbb{F}}_p$, we have the commutative diagram of ℓ -divisible groups over $\overline{\mathbb{F}}_p$*

$$(4.6) \quad \begin{array}{ccc} A_0(\ell) \otimes \overline{\mathbb{F}}_p & \xrightarrow{f} & A_0(\ell) \otimes \overline{\mathbb{F}}_p \\ \downarrow \pi_0 & & \downarrow \pi_0 \\ A_0(\ell) \otimes \overline{\mathbb{F}}_p & \xrightarrow{\sigma_p(f)} & A_0(\ell) \otimes \overline{\mathbb{F}}_p. \end{array}$$

- (3) *For any prime $\ell \neq p$, any endomorphism f of the Tate module $T_\ell(A_0)$ and any element $\sigma \in \mathcal{G}$, we have the commutative diagram of Tate modules*

$$(4.7) \quad \begin{array}{ccc} T_\ell(A_0) & \xrightarrow{f} & T_\ell(A_0) \\ \downarrow \sigma & & \downarrow \sigma \\ T_\ell(A_0) & \xrightarrow{\sigma(f)} & T_\ell(A_0). \end{array}$$

PROOF. The statements (1) and (2) follow immediately from the second commutative diagram in (4.2). The statement (3) follows immediately from the commutative diagram (2.15) by letting $S = T = \text{Spec } \overline{\mathbb{F}}_p$ and $\tau = \sigma^*$ and taking the projective limit. ■

4.4. **An example.** We show that there is a p -divisible group X over an algebraically closed field k such that X is not isomorphic to ${}^\sigma X$ for some automorphism σ of k . Let E_0 be a supersingular p -divisible group of rank 2 over \mathbb{F}_{p^2} such that the relative Frobenius morphism (from $E_0 \rightarrow E_0^{(p^2)} = E_0$) is equal to the morphism $[-p]$. Let $X_0 := E_0^2$. The functor

$$\mathcal{P} : (\mathbb{F}_{p^2}\text{-schemes}) \rightarrow (\text{sets}), \quad \mathcal{P}(T) := \text{Hom}_T(\alpha_p \times T, X_0 \times T)$$

is representable by the projective line \mathbf{P}^1 over \mathbb{F}_{p^2} . Since any morphism $\varphi \in \text{Hom}_T(\alpha_p \times T, X_0 \times T)$ factors through the morphism $(\alpha_p \times \alpha_p) \times T \rightarrow X_0 \times T$, the group $\text{End}_{\mathbb{F}_{p^2}}(\alpha_p^2)^\times = \text{GL}_2(\mathbb{F}_{p^2})$ acts naturally on the projective line from the left. For any point $\varphi = [a : b] \in \mathbf{P}^1(k)$, we write $X_{[a:b]}$ for the quotient p -divisible group $X_0/\varphi(\varphi)$.

Lemma 4.4. *Two p -divisible groups $X_{[a:b]}$ and $X_{[a':b']}$ are isomorphic over k if and only if there is an element $h \in \text{GL}_2(\mathbb{F}_{p^2})$ such that $h[a : b] = [a' : b']$.*

We leave this as an exercise to the reader. Take $k = \overline{\mathbb{F}_p}(t)$. Let $b \in k$ be any element such that $[1 : b] \notin \mathrm{GL}_2(\mathbb{F}_{p^2})[1 : t]$. Let $\sigma \in \mathrm{Aut}(k)$ be an automorphism which sends t to b . Then the p -divisible group ${}^\sigma X_{[1:t]} = X_{[1:b]}$ is not isomorphic to $X_{[1:t]}$ over k .

4.5. Relationship between p -divisible groups X and ${}^\sigma X$. Let c, d be two positive integers. Let $p\text{-div}(d, c)(k)$ be the set of isomorphism classes of p -divisible groups X of dimension d and of co-dimension c over a field k of characteristic p . By a p -adic invariant ψ we mean the association to the equivalence class for an equivalent relation \sim on $p\text{-div}(d, c)(k)$ that is defined using the morphisms F^m , V^n and $[p^r]$, for some integers m, n, r . For any two p -divisible groups $X_1, X_2 \in p\text{-div}(d, c)(k)$, we write $\psi(X_1) = \psi(X_2)$ if $X_1 \sim X_2$. Examples of equivalence relations (over an algebraically closed field) are:

- (i) Define $X_1 \sim X_2$ if X_1 is isogenous to X_2 . In this case, the p -adic invariant ψ is the association to X its Newton polygon $NP(X)$.
- (ii) Define $X_1 \sim X_2$ if there is an isomorphism $X_1[p] \simeq X_2[p]$. In this case, the p -adic invariant ψ is the association to X its EO type $ES(X)$; see Oort [22] for detail descriptions of EO types.
- (iii) Define $X_1 \sim X_2$ if there is an isomorphism $X_1 \simeq X_2$. In this case, the p -adic invariant ψ is the association to X the isomorphism class of itself.

A p -adic invariant ψ is said to be *discrete* if the image

$$\Psi(k) := \{\psi(X); X \in p\text{-div}(d, c)(k)\}$$

is finite for any algebraically closed field $k \supset \mathbb{F}_p$. The p -adic invariants in (i) and (ii) are discrete, while the p -adic invariant in (iii) is not.

Theorem 4.5. *Let ψ be a discrete p -adic invariant on the set $p\text{-div}(d, c)(k)$, where k is an algebraically closed field of characteristic p . Then there is a p -power integer $q \in \mathbb{N}$ such that*

$$\psi(X) = \psi({}^\sigma X)$$

for all $X \in p\text{-div}(d, c)(k)$ and $\sigma \in \mathrm{Gal}(k/\mathbb{F}_q)$.

PROOF. Since ψ is discrete, there is a p -power integer $q \in \mathbb{N}$ such that for any $X \in p\text{-div}(d, c)(k)$, there is a p -divisible group X_0 over \mathbb{F}_q such that

$$\psi(X) = \psi(X_0 \otimes_{\mathbb{F}_q} k)$$

(otherwise $\Psi(\overline{\mathbb{F}_p})$ would be infinite). We apply any element $\sigma \in \mathrm{Gal}(k/\mathbb{F}_q)$ and get $\psi({}^\sigma X) = \psi(X_0 \otimes_{\mathbb{F}_q} k)$. Then the assertion follows. ■

Due to a counterexample in Section 4.4, Theorem 4.5 seems to be the best we can hope for about the relationship between the p -divisible groups X and ${}^\sigma X$.

5. GALOIS ACTION ON Λ_g AND PROOF OF THEOREM 1.1

5.1. Let $\underline{A}_0 = (A_0, \lambda_0)$ be a g -dimensional superspecial principally polarized abelian variety over \mathbb{F}_p . Recall that to the polarized abelian variety \underline{A}_0 we associate two group schemes $G_1 \subset G$ over \mathbb{Z} as follows. For any commutative ring R , the groups of their R -valued points are defined as

$$G(R) := \{x \in (\mathrm{End}_{\overline{\mathbb{F}_p}}(A_0 \otimes \overline{\mathbb{F}_p}) \otimes R)^\times \mid x'x \in R^\times\},$$

$$G_1(R) := \{x \in (\text{End}_{\overline{\mathbb{F}}_p}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes R)^\times \mid x'x = 1\},$$

where the map $x \mapsto x'$ is the Rosati involution induced by the polarization λ_0 . Let $\nu : G \rightarrow \mathbb{G}_m$ be the multiplier character; we have $\ker \nu = G_1$. Recall that σ_p denotes the arithmetic Frobenius element in the Galois group $\mathcal{G} = \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ and π_0 is the relative Frobenius morphism of A_0 over \mathbb{F}_p .

Lemma 5.1. *We have $\pi_0 \in G(\mathbb{Q})$.*

PROOF. Choose any prime $\ell \neq p$. The polarization λ_0 induces the Weil pairing $e_\ell : T_\ell(A_0) \times T_\ell(A_0) \rightarrow \mathbb{Z}_\ell(1)$, which is \mathcal{G} -equivariant. Then we have (cf. Proposition 4.3 (2) and (3))

$$e_\ell(\pi x, \pi y) = e_\ell(\sigma_p x, \sigma_p y) = p e_\ell(x, y).$$

Since $G(\mathbb{Q}) \subset G(\mathbb{Q}_\ell)$, this shows that $\pi'_0 \pi_0 = p$ and hence the lemma. ■

Proposition 5.2. *The action of \mathcal{G} on $G(\mathbb{A}_f)$ is given by*

$$(5.1) \quad \sigma_p(x_\ell)_\ell = (\pi_0 x_\ell \pi_0^{-1})_\ell, \quad (x_\ell)_\ell \in G(\mathbb{A}_f).$$

PROOF. It suffices to show that for any prime ℓ (including p), the action of \mathcal{G} on $\text{End}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes \mathbb{Z}_\ell$ is given by

$$(5.2) \quad \sigma_p x_\ell = \pi_0 x_\ell \pi_0^{-1}, \quad x_\ell \in \text{End}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes \mathbb{Z}_\ell.$$

Since A_0 is supersingular, we have the natural isomorphism

$$\text{End}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes \mathbb{Z}_\ell \simeq \text{End}(A(\ell) \otimes \overline{\mathbb{F}}_p).$$

The relation (5.2) then follows from Proposition 4.3 (2). This shows the proposition. ■

5.2. We now describe the map

$$\mathbf{d}_1 : G_1(\mathbb{Q}) \backslash G_1(\mathbb{A}_f) / G_1(\hat{\mathbb{Z}}) \simeq \Lambda_g$$

and show that it is \mathcal{G} -equivariant. We introduce the following notations.

Notations. Let k be any field. Let ℓ be a prime, not necessarily invertible in k . For any object $\underline{A} = (A, \lambda)$ in \mathcal{A}_g over k , we write $\underline{A}(\ell) := (A, \lambda)[\ell^\infty]$ for the associated ℓ -divisible group with the induced quasi-polarization. For any two members $\underline{A}_1 = (A_1, \lambda_1)$ and $\underline{A}_2 = (A_2, \lambda_2)$ in \mathcal{A}_g over k , denote by

- $\text{Isog}_k(\underline{A}_1, \underline{A}_2)$ (resp. $\text{Isom}_k(\underline{A}_1, \underline{A}_2)$) the set of quasi-isogenies (resp. isomorphisms) $\varphi : A_1 \rightarrow A_2$ over k such that $\varphi^* \lambda_2 = \lambda_1$, and
- $\text{Isog}_k(\underline{A}_1(\ell), \underline{A}_2(\ell))$ (resp. $\text{Isom}_k(\underline{A}_1(\ell), \underline{A}_2(\ell))$) the set of quasi-isogenies (resp. isomorphisms) $\varphi : A_1[\ell^\infty] \rightarrow A_2[\ell^\infty]$ such that $\varphi^* \lambda_2 = \lambda_1$.

Proposition 5.3. *Let $(\phi_\ell)_\ell \in G_1(\mathbb{A}_f)$ be an element. Then there exist*

- a member $\underline{A} = (A, \lambda) \in \Lambda_g$ determined up to isomorphism,
- a quasi-isogeny $\phi \in \text{Isog}_{\overline{\mathbb{F}}_p}(\underline{A}, \underline{A}_0)$, and
- an isomorphism $\alpha_\ell \in \text{Isom}_{\overline{\mathbb{F}}_p}(\underline{A}_0(\ell), \underline{A}(\ell))$ for each ℓ

such that $\phi_\ell = \phi \circ \alpha_\ell$ for all ℓ . Moreover, the map $\tilde{\mathbf{d}}_1 : G_1(\mathbb{A}_f) \rightarrow \Lambda_g$ which sends $(\phi_\ell)_\ell$ to the isomorphism class $[\underline{A}]$ induces a well-defined and bijective map

$$\mathbf{d}_1 : G_1(\mathbb{Q}) \backslash G_1(\mathbb{A}_f) / G_1(\hat{\mathbb{Z}}) \simeq \Lambda_g.$$

PROOF. See [33, Theorem 10.5] or [37, Theorem 2.2].

Let $(\phi_\ell)_\ell \in G_1(\mathbb{A}_f)$ be an element, and let \underline{A} , ϕ , α_ℓ be as above. Applying an element σ in \mathcal{G} , we get

$$\sigma(\phi) \in \text{Isog}_{\overline{\mathbb{F}}_p}({}^\sigma \underline{A}, \underline{A}_0), \quad \sigma(\alpha_\ell) \in \text{Isom}_{\overline{\mathbb{F}}_p}(\underline{A}_0(\ell), {}^\sigma \underline{A}(\ell))$$

and

$$\sigma(\phi_\ell) = \sigma(\phi) \circ \sigma(\alpha_\ell), \quad \forall \ell.$$

This yields $\tilde{\mathbf{d}}_1(\sigma(\phi_\ell)_\ell) = [{}^\sigma \underline{A}]$, and hence the map $\tilde{\mathbf{d}}_1$ is \mathcal{G} -equivariant.

The inclusion $G_1(\mathbb{A}_f) \rightarrow G(\mathbb{A}_f)$ is \mathcal{G} -equivariant and it induces a \mathcal{G} -equivariant bijection

$$G_1(\mathbb{Q}) \backslash G_1(\mathbb{A}_f) / G_1(\hat{\mathbb{Z}}) \simeq G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / G(\hat{\mathbb{Z}}).$$

Let

$$\tilde{\mathbf{d}} : G(\mathbb{A}_f) \rightarrow G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / G(\hat{\mathbb{Z}}) \simeq G_1(\mathbb{Q}) \backslash G_1(\mathbb{A}_f) / G_1(\hat{\mathbb{Z}}) \xrightarrow{\mathbf{d}_1} \Lambda_g$$

be the composition. We have shown

Proposition 5.4. *The induced map $\tilde{\mathbf{d}} : G(\mathbb{A}_f) \rightarrow \Lambda_g$ is \mathcal{G} -equivariant.*

Theorem 1.1 is proved.

5.3. Relation with the Atkin-Lehner involution. Let $\underline{A}_0 = (A_0, \lambda_0)$ be as in Section 5.1. Assume that the relative Frobenius morphism π_0 satisfying $\pi_0^2 = -p$. Such an object exists; for example, see [10, Section 1], or apply the Honda-Tate theory to the Weil number $\sqrt{-p}$ (see [30]). Let $B_{p,\infty}$ denote the quaternion algebra over \mathbb{Q} ramified exactly at p and ∞ . For a suitable identification $\text{End}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes \mathbb{Q} \simeq M_g(B_{p,\infty}) \subset M_{2g}(\mathbb{Q}(\sqrt{-p}))$ with respect to the Rosati involution, the element π_0 is represented by the matrix

$$\begin{pmatrix} 0 & -pI_g \\ I_g & 0 \end{pmatrix},$$

where I_g is the $g \times g$ identity matrix. The action of Frobenius element σ_p on $G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / G(\hat{\mathbb{Z}})$, according to Proposition 5.2, is an involution of Atkin-Lehner type.

6. PROOF OF THEOREMS 1.2 AND 1.3

From now on, we fix the base point (A_0, λ_0) over \mathbb{F}_p so that $A_0 = E_0^g$, where E_0 is a supersingular elliptic curve over \mathbb{F}_p satisfying $\pi_{E_0}^2 = -p$, and λ_0 is the product of copies of the canonical polarization on E_0 . Let G be the group scheme over \mathbb{Z} associated to the polarized abelian variety (A_0, λ_0) as in Section 1 (and Section 5.1).

6.1. Proof of Theorems 1.2 and 1.3 (1).

Proposition 6.1. *Every member (A, λ) in Λ_g has a unique model defined over \mathbb{F}_{p^2} , up to isomorphism over \mathbb{F}_{p^2} , such that the quasi-isogeny ϕ in Proposition 5.3 can be chosen defined over \mathbb{F}_{p^2} .*

PROOF. This refines [10, Lemma 2.1]. Let $(\phi_\ell) \in G_1(\mathbb{A}_f)$ be an element such that the class $[(\phi_\ell)]$ corresponds to (A, λ) . Let ϕ and α_ℓ for all ℓ be as in Proposition 5.3. If $\sigma \in \text{Gal}(\overline{\mathbb{F}}_p / \mathbb{F}_{p^2})$, then by Theorem 1.1 we have $\sigma(\phi) \circ \sigma(\alpha_\ell) = \phi \circ \alpha_\ell$, and hence $\phi_\sigma := \phi^{-1} \circ \sigma(\phi) : ({}^\sigma A, {}^\sigma \lambda) \rightarrow (A, \lambda)$ is an isomorphism. For $\sigma, \tau \in \text{Gal}(\overline{\mathbb{F}}_p / \mathbb{F}_{p^2})$, put $f_{\tau, \sigma} = \phi_\tau^{-1} \circ \phi_\sigma : ({}^\sigma A, {}^\sigma \lambda) \simeq ({}^\tau A, {}^\tau \lambda)$. Then it is easy to check that the conditions

(i) and (ii) of Theorem 3.1 for $f_{\tau,\sigma}$ are satisfied. Therefore by Weil's Theorem, there are a model (A_1, λ_1) over \mathbb{F}_{p^2} and an isomorphism $f : (A_1, \lambda_1) \otimes_{\mathbb{F}_{p^2}} \overline{\mathbb{F}_p} \simeq (A, \lambda)$ such that $\phi_\sigma = f \circ \sigma(f)^{-1}$. We get $\sigma(\phi \circ f) = \phi \circ f$, and hence $\phi_1 := \phi \circ f$ is a quasi-isogeny in $\text{Isog}_{\mathbb{F}_{p^2}}(\underline{A}_1, \underline{A}_0)$.

Suppose that (A_2, λ_2) is another model over \mathbb{F}_{p^2} of (A, λ) such that the set $\text{Isog}_{\mathbb{F}_{p^2}}(\underline{A}_2, \underline{A}_0)$ is non-empty. Then we can choose $\phi_2 \in \text{Isog}_{\mathbb{F}_{p^2}}(\underline{A}_2, \underline{A}_0)$ such that $\phi_2^{-1}\phi_1 : \underline{A}_1 \rightarrow \underline{A}_2$ is an isomorphism, which is defined over \mathbb{F}_{p^2} . This shows the proposition. ■

Let \mathbf{A}_g denote the coarse moduli scheme over \mathbb{F}_p for the moduli space \mathcal{A}_g . We also regard $\Lambda_g \subset \mathbf{A}_g$ as the closed subscheme over \mathbb{F}_p with the induced reduced structure. Therefore, for any subfield k_0 of $\overline{\mathbb{F}_p}$, the set $\Lambda_g(k_0)$ of k_0 -points in Λ_g equals the subset of fixed elements by $\text{Gal}(\overline{\mathbb{F}_p}/k_0)$, or the same, the subset consisting of objects (A, λ) in Λ_g whose isomorphism classes are defined over k_0 . This particularly defines the subset $\Lambda_g(\mathbb{F}_p)$ of Λ_g .

It follows from Theorem 1.1 that $\Lambda_g(\mathbb{F}_{p^2}) = \Lambda_g$. Proposition 6.1 allows us to identify $\Lambda_g(\mathbb{F}_{p^2})$ with the set of isomorphism classes of g -dimensional superspecial principally polarized abelian varieties (A_1, λ_1) over \mathbb{F}_{p^2} (classified up to isomorphism over \mathbb{F}_{p^2} , not over $\overline{\mathbb{F}_p}$) such that the set $\text{Isog}_{\mathbb{F}_{p^2}}(\underline{A}_1, \underline{A}_0)$ (see Section 5.2) is non-empty. We shall call the unique model \underline{A}_1 obtained in Proposition 6.1 the *canonical model* of (A, λ) over \mathbb{F}_{p^2} . Note that if \underline{A}_1 is a canonical model over \mathbb{F}_{p^2} , then the relative Frobenius morphism $\pi_{A_1/\mathbb{F}_{p^2}}$ is equal to $-p$ and hence every endomorphism in $\text{End}_{\overline{\mathbb{F}_p}}(A_1)$ is defined over \mathbb{F}_{p^2} .

Recall that $U := G(\hat{\mathbb{Z}}) \subset G(\mathbb{A}_f)$ and $U(\pi_0) := U\pi_0 = \pi_0 U \subset G(\mathbb{A}_f)$ are open compact subgroups.

Proposition 6.2.

- (1) *Let (A, λ) be a member in Λ_g and let $[x] \in G(\mathbb{Q}) \backslash G(\mathbb{A}_f)/U$ be the double coset corresponding to $[(A, \lambda)]$. Then (A, λ) lies in $\Lambda_g(\mathbb{F}_p)$ if and only if*

$$(6.1) \quad G(\mathbb{Q}) \cap xU(\pi_0)x^{-1} \neq \emptyset.$$

- (2) *We have $|\Lambda(\mathbb{F}_p)| = \text{tr } R(\pi_0)$.*

PROOF. (1) The isomorphism class of (A, λ) is fixed by σ_p exactly when $[x] = [\pi_0 x \pi_0^{-1}] = [x \pi_0]$. Therefore, there are some elements $u \in U$ and $a \in G(\mathbb{Q})$ such that $x = ax \pi_0 u$. We get $a^{-1} = x \pi_0 u x^{-1}$. This is equivalent to the condition (6.1).

(2) By Theorem 1.1, $R(\pi_0)$ is the operator induced by the action of σ_p^{-1} . Therefore, the number of fixed points of σ_p is equal to $\text{tr } R(\pi_0)$. This shows the proposition. ■

Proposition 6.3. *Let (A, λ) be polarized abelian variety over $\overline{\mathbb{F}_p}$, and suppose that the field of moduli of (A, λ) is \mathbb{F}_{p^a} . Then (A, λ) has a model defined over \mathbb{F}_{p^a} .*

PROOF. Put $q := p^a$ and let $\sigma : x \mapsto x^q$ be the Frobenius automorphism in $\text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_q)$. Suppose (A, λ) has a model (A_1, λ_1) defined over \mathbb{F}_{q^c} for some positive integer c divisible by a . Increasing c if necessary, we may assume that $\text{End}_{\overline{\mathbb{F}_p}}(A) = \text{End}_{\mathbb{F}_{p^c}}(A_1)$. Under the assumption, there is an isomorphism

$$a_\sigma : (A, \lambda) \simeq (\sigma A, \sigma \lambda)$$

of polarized abelian varieties over $\overline{\mathbb{F}}_p$. Let

$$b_\sigma := \sigma^{c-1}(a_\sigma) \cdots \sigma(a_\sigma) a_\sigma : (A, \lambda) \rightarrow (A, \lambda)$$

be the composition. Since b_σ is an automorphism of (A, λ) , it is of finite order, say $b_\sigma^m = 1$ for some $m \geq 1$. It follows from $\text{End}(A) = \text{End}(A_0)$ that $\sigma^c(b_\sigma) = b_\sigma$. We get

$$(6.2) \quad \sigma^{mc-1}(a_\sigma) \cdots \sigma(a_\sigma) a_\sigma = 1.$$

Define $a_{\sigma^n} := \sigma(a_{\sigma^{n-1}}) a_\sigma$ recursively. The collection of automorphisms a_{σ^n} satisfies the 1-cocycle condition for the Galois extension $\mathbb{F}_{q^{mc}}/\mathbb{F}_q$, by (6.2). Then by Weil's criterion (Theorem 3.1), there are an abelian variety A' over \mathbb{F}_q and an isomorphism $f : A' \otimes \overline{\mathbb{F}}_p \simeq A$ such that $a_\sigma = \sigma(f) \circ f^{-1}$. Set $\lambda' := f^* \lambda$. Using $\lambda = a_\sigma^* \sigma(\lambda)$, we get

$$(6.3) \quad \begin{aligned} \lambda' &= f^t \lambda f = f^t (a_\sigma^* \sigma(\lambda)) f \\ &= f^t a_\sigma^* \sigma(\lambda) a_\sigma f = \sigma(f^t) \sigma(\lambda) \sigma(f) = \sigma(\lambda'). \end{aligned}$$

This shows that (A', λ') is a model defined over \mathbb{F}_q of (A, λ) . ■

Corollary 6.4. *Let (A, λ) be a member in Λ_g . If the field of moduli of (A, λ) is equal to \mathbb{F}_p , then (A, λ) has a model defined by \mathbb{F}_p . That is, the set $\Lambda_g(\mathbb{F}_p) \subset \Lambda_g$ consists of objects that have a model defined over \mathbb{F}_p .*

Theorems 1.2 and 1.3 (1) follows from Propositions 6.1, 6.2 and Corollary 6.4.

We remark that the same proof of Proposition 6.3 also shows the following generalization:

Proposition 6.5. *Let (X, ξ) be an (irreducible) variety over $\overline{\mathbb{F}}_p$ together with an additional structure ξ which is defined algebraically. If the automorphism group $\text{Aut}_{\overline{\mathbb{F}}_p}(X, \xi)$ is finite and assume that the Weil descent datum for (X, ξ) is effective, then (X, ξ) has a model defined over the field of moduli of (X, ξ) .*

When X is quasi-projective and ξ is a polarization (an algebraic equivalence class of an ample line bundle) and/or a morphism in $\text{Mor}(X^m, X^n)$, where $X^m = X \times_k \cdots \times_k X$ is the m -fold fiber product of X , the assumption of the Weil descent datum holds for (X, ξ) .

6.2. Proof of Theorem 1.3 (2). Let D be the group scheme over \mathbb{Z} which representing the following functor

$$R \rightarrow (\text{End}_{\overline{\mathbb{F}}_p}(E_0) \otimes R)^\times,$$

where R is a commutative ring. In particular, $D(\mathbb{Q}_p) = (B_{p,\infty} \otimes \mathbb{Q}_p)^\times$. We regard D as a subgroup scheme of G through the diagonal embedding. Let Z be the center of G .

Lemma 6.6.

- (1) *For any prime $\ell \neq p$, the subgroup N_ℓ of $G(\mathbb{Q}_\ell)$ which normalizes the maximal order $\text{End}_{\overline{\mathbb{F}}_p}(A_0) \otimes \mathbb{Z}_\ell$ is $Z(\mathbb{Q}_\ell)G(\mathbb{Z}_\ell)$.*
- (2) *The subgroup N_p of $G(\mathbb{Q}_p)$ which normalizes the maximal order $\text{End}_{\overline{\mathbb{F}}_p}(A_0) \otimes \mathbb{Z}_p$ is $D(\mathbb{Q}_p)G(\mathbb{Z}_p)$.*

PROOF. We sketch the proof; the omitted part is mere straightforward computation. Put $H_\ell := Z(\mathbb{Q}_\ell)G(\mathbb{Z}_\ell)$, for $\ell \neq p$, and $H_p := D(\mathbb{Q}_p)G(\mathbb{Z}_p)$. It is clear that the group H_v normalizes the order $\mathcal{O}_v := \text{End}_{\mathbb{F}_p}(A_0) \otimes \mathbb{Z}_v$. It suffices to show that any element \bar{g} in N_v/H_v is the identity class. By the Iwasawa decomposition, we have $G(\mathbb{Q}_v) = P(\mathbb{Q}_v)G(\mathbb{Z}_v)$, where P is the standard minimal parabolic subgroup over \mathbb{Q}_v . We may assume that a representative g_ℓ (resp. g_p) is a upper triangular matrix in $G(\mathbb{Q}_\ell) \subset M_{2g}(\mathbb{Q}_\ell)$ (resp. in $G(\mathbb{Q}_p) \subset M_g(B_{p,\infty} \otimes \mathbb{Q}_p)$). Let E_{ij} denote the matrix in which the (i, j) -entry is 1 and others are zero. It follows from $g_v E_{ij} g_v^{-1} \in \mathcal{O}_v$ for all i, j (by looking at its (i, j) -entry) that the diagonal entries of g_v have the same valuation. Modulo H_v , we may assume that g_v lies in the group of upper triangular unipotent matrices. It follows from $g_v E_{ii} g_v^{-1} \in \mathcal{O}_v$ for all i that every entry of g_v is integral and hence $g_v \in G(\mathbb{Z}_v)$. This shows the lemma. ■

Remark 6.7. One can also use the Cartan decomposition to show Lemma 6.6.

Let \tilde{U} be the open subgroup of $G(\mathbb{A}_f)$ generated by the open compact subgroup U and the element π_0 . Since π_0 normalizes U and $\pi_0^m \notin U$ for $m \neq 0$, we have

$$\tilde{U} = \bigcup_{m \in \mathbb{Z}} U \pi_0^m, \quad (\text{disjoint}).$$

Consider $G(\mathbb{Q})$ as a subgroup of $G(\mathbb{Q}_v)$ for each place v and identify π_0 with its image in $G(\mathbb{Q}_v)$. Note that $\pi_0 \in G(\mathbb{Z}_\ell)$ for $\ell \neq p$, and $\pi_0 \in D(\mathbb{Q}_p)$, which is also a uniformizer of the division quaternion algebra $B_{p,\infty} \otimes \mathbb{Q}_p$. We have

$$\tilde{U} = \tilde{U}_p \times U^p, \quad \tilde{U}_p = \bigcup_{m \in \mathbb{Z}} G(\mathbb{Z}_p) \pi_0^m = D(\mathbb{Q}_p)G(\mathbb{Z}_p),$$

where $U^p = \prod_{\ell \neq p} G(\mathbb{Z}_\ell)$.

Corollary 6.8. *Notations as above. The natural map*

$$G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / \tilde{U} \rightarrow \mathcal{T}(G) = G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / \mathfrak{N}$$

is bijective.

PROOF. By Lemma 6.6, we have

$$G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / \mathfrak{N} = G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / (\tilde{U}_p \times Z(\mathbb{A}_f^p) U^p),$$

where \mathbb{A}_f^p is the ring of prime-to- p finite adeles of \mathbb{Q} . The latter is equal to

$$G(\mathbb{Q})(\{1\} \times Z(\mathbb{A}_f^p)) \backslash G(\mathbb{A}_f) / (\tilde{U}_p \times U^p) = G(\mathbb{Q})(\{1\} \times Z(\hat{\mathbb{Z}}^p)) \backslash G(\mathbb{A}_f) / \tilde{U}.$$

Since $Z(\hat{\mathbb{Z}}^p) \subset U^p$, the latter is equal to $G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / \tilde{U}$. This finishes the proof. ■

Theorem 6.9. *The natural projection $\text{pr} : G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / U = \Lambda_g \rightarrow \mathcal{T}(G)$ induces a bijection between the set of orbits of Λ_g under the action of $\text{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ with the set $\mathcal{T}(G)$.*

PROOF. By Corollary 6.8, the map $\Lambda_g \rightarrow \mathcal{T}(G)$ is simply the projection map $\text{pr} : G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / U \rightarrow G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / \tilde{U}$, and the Frobenius $\sigma_p = \sigma_p^{-1}$ acts as $[x] \mapsto [x\pi_0]$ for $x \in G(\mathbb{A}_f)$. Since π_0 normalizes U , we have $\text{pr}([x]) = \text{pr}([x\pi_0])$. Suppose $\text{pr}([x]) = \text{pr}([y])$ for $x, y \in G(\mathbb{A}_f)$. Then $y = ax\pi_0^m u$ for some $m \in \mathbb{Z}$, $u \in U$ and $a \in G(\mathbb{Q})$. Since $\pi_0^2 = -p$ is in the center, we may assume $m = 0$ or 1 . Then $[y] = [x\pi_0^m]$ for $m = 0$ or 1 . This completes the proof. ■

Let $\Lambda'_g := \Lambda(\mathbb{F}_p)^c$ be the complement of $\Lambda(\mathbb{F}_p)$ in Λ_p . Theorem 6.9 shows that

$$(6.4) \quad \frac{1}{2}|\Lambda'_g| + |\Lambda_g(\mathbb{F}_p)| = T.$$

By $H = |\Lambda_g| = |\Lambda'_g| + |\Lambda_g(\mathbb{F}_p)|$ and $\text{tr } R(\pi_0) = |\Lambda_g(\mathbb{F}_p)|$, we get

$$\text{tr } R(\pi_0) = 2T - H.$$

Theorem 1.3 (2) is proved.

Remark 6.10. We discuss a bit some relationship between Proposition 6.1 and Corollary 6.4. We call a model (A', λ') over \mathbb{F}_p of a member (A, λ) in $\Lambda_g(\mathbb{F}_p)$ *nearly canonical* if the set $\text{Isog}_{\mathbb{F}_{p^2}}(\underline{A}', \underline{A}_0)$ is non-empty, that is, the base change $(A', \lambda') \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$ is the canonical model over \mathbb{F}_{p^2} in the sense of Proposition 6.1. We do not know whether or not any member (A, λ) in $\Lambda_g(\mathbb{F}_p)$ admits a model over \mathbb{F}_p which is nearly canonical. The object (A, λ) admits a nearly canonical model over \mathbb{F}_p if and only if one can choose an automorphism $a_{\sigma_p} : (A, \lambda) \simeq (\sigma_p A, \sigma_p \lambda)$ such that $\sigma_p(a_{\sigma_p})a_{\sigma_p} = 1$.

On the other hand, it is possible that an object in $\Lambda_g(\mathbb{F}_p)$ may admit a model over \mathbb{F}_p which is not nearly canonical. We give an example.

Consider the case $g = 1$. Take a supersingular elliptic curve E over \mathbb{F}_p such that its Frobenius endomorphism π_E does not satisfy $\pi_E^2 + p = 0$ (this is only possible when $p = 2$ or $p = 3$). Then E is not a nearly canonical model in its isomorphism class over $\overline{\mathbb{F}}_p$. However, when $p > 3$ every elliptic curve over \mathbb{F}_p is a nearly canonical model in its isomorphism class over $\overline{\mathbb{F}}_p$.

7. VARIANTS WITH LEVEL STRUCTURES

In this section, the ground field for abelian varieties, if not specified, is always $\overline{\mathbb{F}}_p$.

7.1. We keep the notations as before. Let N be a prime-to- p positive integer. Let U_N^p be the kernel of the reduction map $G(\hat{\mathbb{Z}}^{(p)}) \rightarrow G(\mathbb{Z}/N\mathbb{Z})$, $U_p := G(\mathbb{Z}_p)$, and $U_N := U_p \times U_N^p$, where $\hat{\mathbb{Z}}^{(p)} := \prod_{\ell \neq p} \mathbb{Z}_\ell$.

Denote by $\Lambda_{g,N}^* = \Lambda_{g,N}^*(\overline{\mathbb{F}}_p)$ the set of isomorphism classes of objects (A, λ, η_N) over $\overline{\mathbb{F}}_p$, where

- $(A, \lambda) \in \mathcal{A}_g(\overline{\mathbb{F}}_p)$ is a superspecial point, and
- $\eta_N : A_0[N] \simeq A[N]$ is an isomorphism over $\overline{\mathbb{F}}_p$ such that there is an automorphism $\zeta \in \text{Aut}_{\overline{\mathbb{F}}_p}(\mu_N) = (\mathbb{Z}/N\mathbb{Z})^\times$ such that

$$(7.1) \quad e_\lambda(\eta(x), \eta(y)) = \zeta e_{\lambda_0}(x, y), \quad \forall x, y \in A_0[N],$$

where $e_\lambda : A[N] \times A[N] \rightarrow \mu_N$ denotes the Weil pairing induced by the polarization λ .

Two objects (A, λ, η_N) and (A', λ', η'_N) are isomorphic, denoted as $(A, \lambda, \eta_N) \simeq (A', \lambda', \eta'_N)$, if there is an isomorphism $\varphi : A \rightarrow A'$ such that $\varphi^* \lambda' = \lambda$ and $\varphi_* \eta_N = \eta'_N$. We call η_N above a *level- N structure on (A, λ) with respect to \underline{A}_0* (over $\overline{\mathbb{F}}_p$).

For any prime ℓ , let

$$\text{GIsom}(\underline{A}_0(\ell), \underline{A}(\ell))$$

denote the set of isomorphisms $\eta : A_0[\ell^\infty] \rightarrow A[\ell^\infty]$ (over $\overline{\mathbb{F}}_p$) such that $\eta^* \lambda = \zeta \lambda_0$ for some $\zeta \in \mathbb{Z}_\ell^\times$; it is a right $G(\mathbb{Z}_\ell)$ -torsor (The word “G” stands for preserving the

(quasi-)polarizations up to scalars. Compare the definitions $\text{Isog}(\cdot, \cdot)$ in Section 5.2 and $\text{G-isog}(\cdot, \cdot)$ in Section 7.2). For such η , one has

$$(7.2) \quad e_\lambda(\eta(x), \eta(y)) = \zeta e_{\lambda_0}(x, y), \quad \forall x, y \in A_0[\ell^m], \quad \forall m \geq 1 \in \mathbb{Z}.$$

If η is an element in $\prod_\ell \text{GIsom}(\underline{A}_0(\ell), \underline{A}(\ell))$, where ℓ runs over all primes in \mathbb{Q} , then the restriction $\eta|_{A_0[N]}$ of η to $A_0[N]$ is a level- N structure on (A, λ) with respect to \underline{A}_0 . Conversely, we have

Lemma 7.1. *Any level- N structure η_N on a superspecial object (A, λ) with respect to \underline{A}_0 can be lifted to an element η in $\prod_\ell \text{GIsom}(\underline{A}_0(\ell), \underline{A}(\ell))$.*

PROOF. We may assume that $N = \ell^m$ is a power of ℓ and show that η_N can be lifted in $\text{GIsom}(\underline{A}_0(\ell), \underline{A}(\ell))$, where $\ell \neq p$. Since $\underline{A}_0(\ell)$ is isomorphic to $\underline{A}(\ell)$, we may also assume that $A = A_0$. We have $\text{End}(A_0) \otimes \mathbb{Z}_\ell \simeq \text{End}(A_0(\ell))$, and hence $G(\mathbb{Z}_\ell) = \text{GIsom}(\underline{A}_0(\ell), \underline{A}_0(\ell))$. On the other hand, the group $G(\mathbb{Z}/\ell^m\mathbb{Z})$ consists of elements $\bar{\varphi} \in \text{End}(A_0(\ell)) \otimes (\mathbb{Z}/\ell^m\mathbb{Z})$ such that $\bar{\varphi}'\bar{\varphi} = \zeta \in (\mathbb{Z}/\ell^m\mathbb{Z})^\times$. We shall show the natural map $\text{End}(A_0(\ell)) \otimes \mathbb{Z}/\ell^m\mathbb{Z} \rightarrow \text{End}(A_0[\ell^m])$ is an isomorphism. It then follows that $G(\mathbb{Z}/\ell^m\mathbb{Z})$ is isomorphic to the group of elements $\eta \in \text{End}(A_0[\ell^m])$ such that $\eta^*e_{\lambda_0} = \zeta e_{\lambda_0}$ for some $\zeta \in (\mathbb{Z}/\ell^m\mathbb{Z})^\times$. It follows from the smoothness of G that the reduction map $G(\mathbb{Z}_\ell) \rightarrow G(\mathbb{Z}/\ell^m\mathbb{Z})$ is surjective. Therefore, the element η can be lifted to an element $\varphi \in \text{GIsom}(\underline{A}_0(\ell), \underline{A}_0(\ell))$.

Since $\ell \neq p$, we have $\text{End}(A_0(\ell)) = \text{End}(T_\ell(A_0))$. Since $T_\ell(A_0)$ is a finite free \mathbb{Z}_ℓ -module, we have

$$\text{End}(T_\ell(A_0)) \otimes \mathbb{Z}/\ell^m\mathbb{Z} = \text{End}(T_\ell(A_0)/\ell^m T_\ell(A_0)) = \text{End}(A_0[\ell^m]).$$

This proves the isomorphism $\text{End}(A_0(\ell)) \otimes \mathbb{Z}/\ell^m\mathbb{Z} \simeq \text{End}(A_0[\ell^m])$ and hence the lemma. ■

By Lemma 7.1, each level- N structure η_N on (A, λ) uniquely determines a U_N -orbit

$$[\eta] := \{\eta \in \prod_\ell \text{GIsom}(\underline{A}_0(\ell), \underline{A}(\ell)) \mid \eta|_{A_0[N]} = \eta_N\}$$

in the $G(\hat{\mathbb{Z}})$ -torsor $\prod_\ell \text{GIsom}(\underline{A}_0(\ell), \underline{A}(\ell))$.

Remark 7.2. (1) One can define the notion of level- N structure on an object (A, λ) in Λ_g with respect to \underline{A}_0 as above without the assumption $(p, N) = 1$. However, Lemma 7.1 fails if $p|N$ because the natural map $\text{End}(A_0(p)) \otimes \mathbb{Z}/p^m\mathbb{Z} \rightarrow \text{End}(A_0[p^m])$ is not an isomorphism. For example, let E_0 be a supersingular elliptic curve, then $\text{End}(E_0[p])$ is the algebra

$$\left\{ \begin{pmatrix} a & 0 \\ b & a^p \end{pmatrix} ; a \in \mathbb{F}_{p^2}, b \in \overline{\mathbb{F}}_p \right\},$$

which is not equal to $\text{End}(A_0) \otimes \mathbb{Z}/p\mathbb{Z}$.

(2) For any positive integer N , we call an element

$$[\eta] \in \left[\prod_\ell \text{GIsom}(\underline{A}_0(\ell), \underline{A}(\ell)) \right] / U_N$$

an (\underline{A}_0, U_N) -level structure on the object (A, λ) (see [37, Section 2.2]). This is a better notion of level- N structure on \underline{A} . For any subfield k_0 of $\overline{\mathbb{F}}_p$, an object $(A, \lambda, [\eta])$ over k_0 is defined to be an superspecial principally polarized abelian variety (A, λ)

over k_0 together with an (\underline{A}_0, U_N) -level structure $[\eta]$ on $(A, \lambda) \otimes \overline{\mathbb{F}}_p$ which is invariant under the $\text{Gal}(\overline{\mathbb{F}}_p/k_0)$ -action. One can prove that if the isomorphism class of an objective $(A, \lambda, [\eta])$ over $\overline{\mathbb{F}}_p$ is defined over k_0 , then $(A, \lambda, [\eta])$ admits a model $(A', \lambda', [\eta'])$ over k_0 . The proof is similar to those of Lemma 7.4 and Theorem 7.5 (1).

7.2. For each object $\underline{A} = (A, \lambda) \in \mathcal{A}_g(\overline{\mathbb{F}}_p)$, we write

$$T^{(p)}(A) := \prod_{\ell \neq p} T_\ell(A)$$

for the prime-to- p Tate module of A , and $V^{(p)}(A) := T^{(p)}(A) \otimes_{\mathbb{Z}^{(p)}} \mathbb{A}_f^p$, where \mathbb{A}_f^p is the prime-to- p finite adele ring of \mathbb{Q} . Let

$$\langle \cdot, \cdot \rangle_\lambda : V^{(p)}(A) \times V^{(p)}(A) \rightarrow \mathbb{A}_f^p(1) := V^{(p)}(\mathbb{G}_m)$$

be the induced non-degenerate alternating pairing, for which $T^{(p)}(A)$ is a self-dual $\hat{\mathbb{Z}}^{(p)}$ -lattice. For brevity, we write $V^{(p)}(\underline{A}) := (V^{(p)}(A), \langle \cdot, \cdot \rangle_\lambda)$. We introduce some more notations.

Notations. (1) For any two objects $\underline{A}, \underline{A}'$ in $\mathcal{A}_g(\overline{\mathbb{F}}_p)$, we denote by

$$\text{GIsom}(V^{(p)}(\underline{A}), V^{(p)}(\underline{A}'))$$

the set of isomorphisms $\eta : V^{(p)}(A) \rightarrow V^{(p)}(A')$ such that there is an automorphism $\zeta \in \text{Aut}(\mathbb{A}_f^p(1)) = (\mathbb{A}_f^p)^\times$ such that

$$(7.3) \quad \langle \eta(x), \eta(y) \rangle_{\lambda'} = \zeta \langle \eta(x), \eta(y) \rangle_\lambda, \quad \forall x, y \in V^{(p)}(A).$$

The word ‘‘G’’ stands for preserving polarizations up to scalars.

(2) For any field k and two objects $\underline{A}_1 = (A_1, \lambda_1)$ and $\underline{A}_2 = (A_2, \lambda_2)$ in $\mathcal{A}_g(k)$, denote by $\text{G-isog}_k^{(p)}(\underline{A}_1, \underline{A}_2)$ the set of prime-to- p quasi-isogenies $\varphi : A_1 \rightarrow A_2$ over k such that $\varphi^* \lambda_2 = q \lambda_1$ for some $q \in \mathbb{Z}_{(p),+}^\times$, where $\mathbb{Z}_{(p),+}^\times \subset \mathbb{Z}_{(p)}^\times$ denotes the subset consisting of all positive elements.

Let $\Lambda_{g,N}^{(p)} = \Lambda_{g,N}^{(p)}(\overline{\mathbb{F}}_p)$ denote the set of equivalence classes of objects $(A, \lambda, [\eta]^p)$ over $\overline{\mathbb{F}}_p$, where $(A, \lambda) \in \mathcal{A}_g(\overline{\mathbb{F}}_p)$ is a superspecial point and $[\eta]^p$ is an element in $\text{GIsom}(V^{(p)}(\underline{A}_0), V^{(p)}(\underline{A}))/U_N^p$; two objects $(A, \lambda, [\eta]^p)$ and $(A', \lambda', [\eta']^p)$ are equivalent, denoted as $(A, \lambda, [\eta]^p) \sim (A', \lambda', [\eta']^p)$, if there is a quasi-isogeny $\varphi \in \text{G-isog}_{\overline{\mathbb{F}}_p}^{(p)}((A, \lambda), (A', \lambda'))$ such that $\varphi_*[\eta]^p = [\eta']^p$.

There is a natural map $f : \Lambda_{g,N}^* \rightarrow \Lambda_{g,N}^{(p)}$ which sends each object (A, λ, η_N) to $(A, \lambda, [\eta]^p)$, where $[\eta]^p$ is the class of maps η on $\prod_{\ell \neq p} A_0(\ell)$ whose restriction to $A_0[N]$ is equal to η_N , as we have the identification

$$\begin{aligned} \prod_{\ell \neq p} \text{GIsom}(\underline{A}_0(\ell), \underline{A}(\ell)) &= \text{GIsom}(T^{(p)}(\underline{A}_0), T^{(p)}(\underline{A})) \\ &\subset \text{GIsom}(V^{(p)}(\underline{A}_0), V^{(p)}(\underline{A})). \end{aligned}$$

Theorem 7.3.

- (1) The natural map $f : \Lambda_{g,N}^* \rightarrow \Lambda_{g,N}^{(p)}$ is bijective and compatible with the action of the Galois group \mathcal{G} .

- (2) *There is a natural bijective map $\mathbf{c}_N : \Lambda_{g,N}^{(p)} \rightarrow G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / U_N$ for which the base point $(A_0, \lambda_0, [\text{id}])$ is sent to the identity class $[1]$ and \mathbf{c}_N is \mathcal{G} -equivariant.*

PROOF. (1) Let (A, λ, η_N) and (A', λ', η'_N) be two objects in $\Lambda_{g,N}^*$ such that $(A, \lambda, [\eta]^p) \sim (A', \lambda', [\eta']^p)$. Then there is a prime-to- p quasi-isogeny $\varphi : A \rightarrow A'$ such that $\varphi^* \lambda' = q\lambda$ for some $q \in \mathbb{Z}_{(p),+}^\times$ such that $[\varphi\eta]^p = [\eta']^p$. We may assume $\eta' = \varphi\eta$. As $\eta'\eta^{-1}$ maps $T^{(p)}(A)$ onto $T^{(p)}(A')$, the map $\varphi = \eta'\eta^{-1}$ induces an isomorphism from $T^{(p)}(A)$ to $T^{(p)}(A')$. Therefore, $v_\ell(q) = 0$ for all $\ell \neq p$, and hence we have $\varphi^* \lambda' = \lambda$ and $\varphi\eta_N = \eta'_N$. This shows the injectivity.

We show the surjectivity. Let $(A, \lambda, [\eta]^p)$ be an object in $\Lambda_{g,N}^{(p)}$, where $\eta \in \text{GIsom}(V^{(p)}(\underline{A}_0), V^{(p)}(\underline{A}))$. Let $\zeta \in (\mathbb{A}_f^\times)^\times$ such that $\eta^* \langle \cdot, \cdot \rangle_\lambda = \zeta \langle \cdot, \cdot \rangle_{\lambda_0}$. Choose a positive number $\alpha \in \mathbb{Z}_{(p)}^\times$ so that $\alpha\zeta \in (\hat{\mathbb{Z}}^{(p)})^\times$. Choose a prime-to- p quasi-isogeny φ on A such that $\varphi^* \lambda = \alpha\lambda$. Then $(A, \lambda, [\eta]^p) \sim (A, \lambda, [\varphi\eta]^p)$. Replacing η by $\varphi\eta$, we may assume that $\zeta \in (\hat{\mathbb{Z}}^{(p)})^\times$. Let $L := \eta(T^{(p)}(A_0)) \subset V^{(p)}(A)$ be the image of $T^{(p)}(A_0)$ under η . By a theorem of Tate, there are an abelian variety A' and a prime-to- p quasi-isogeny $\varphi' : A' \rightarrow A$ such that the map φ' induces an isomorphism

$$T^{(p)}(A') \xrightarrow{\varphi'} T^{(p)}(A) \simeq L \subset V^{(p)}(A);$$

the pair (A', φ') is uniquely determined up to isomorphism by this property. Let $\lambda' := \varphi'^* \lambda$, considered as an element in $\text{Hom}(A', (A')^t) \otimes \mathbb{Z}_{(p)}$; one has $\langle \cdot, \cdot \rangle_{\lambda'} = \varphi'^* \langle \cdot, \cdot \rangle_\lambda$. We have the following diagram:

$$\begin{array}{ccc} & T^{(p)}(A_0), \zeta \langle \cdot, \cdot \rangle_{\lambda_0} & \\ \swarrow \varphi'^{-1}\eta & \downarrow \eta & \\ T^{(p)}(A'), \langle \cdot, \cdot \rangle_{\lambda'} & \xrightarrow{\varphi'} & L, \langle \cdot, \cdot \rangle_\lambda \end{array}$$

It follows from $\varphi'^{-1} \circ \eta \in \text{GIsom}(T^{(p)}(\underline{A}_0), T^{(p)}(\underline{A}))$ that λ' is a principal polarization. Then $(A, \lambda, [\eta]^p) \sim (A', \lambda', [\varphi'^{-1} \circ \eta]^p)$ and the latter comes from an element in $\Lambda_{g,N}^*$. This shows the surjectivity. It is obvious that the map f is compatible with the action of \mathcal{G} .

(2) We define the map \mathbf{c}_N . Given an object $(A, \lambda, [\eta]^p)$ in $\Lambda_{g,N}^{(p)}$, there is a prime-to- p quasi-isogeny $\varphi : A \rightarrow A_0$ such that $\varphi^* \lambda_0 = q\lambda$ for some $q \in \mathbb{Z}_{(p),+}^\times$. Then $[\varphi\eta]^p \in G(\mathbb{A}_f^p) / U_N^p$. If φ' is another such a morphism, the $\varphi' = a\varphi$ for some $a \in G(\mathbb{Z}_{(p)})$. Then the map $(A, \lambda, [\eta]^p) \mapsto [\varphi\eta]^p$ induces a well-defined map, denoted by \mathbf{c}_N^p , from $\Lambda_{g,N}^{(p)}$ to $G(\mathbb{Z}_{(p)}) \backslash G(\mathbb{A}_f^p) / U_N^p$. Using the isomorphism $G(\mathbb{Z}_{(p)}) \backslash G(\mathbb{A}_f^p) / U_N^p \simeq G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / U_N$, we get a map

$$\mathbf{c}_N : \Lambda_{g,N}^{(p)} \rightarrow G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / U_N.$$

We need to show that the map \mathbf{c}_N^p is bijective and \mathcal{G} -equivariant. Let $\underline{A} = (A, \lambda, [\eta]^p)$ and $\underline{A}' = (A', \lambda', [\eta']^p)$ be two objects in $\Lambda_{g,N}^{(p)}$, and let φ, φ' be prime-to- p quasi-isogenies to A_0 , respectively. Suppose that $[\varphi\eta]^p = [\varphi'\eta']^p$, that is $\mathbf{c}_N^p(\underline{A}) = \mathbf{c}_N^p(\underline{A}')$. Then the morphism $a := \varphi'^{-1}\varphi : A \rightarrow A'$ is a prime-to- p quasi-isogeny such that $a^* \lambda' \in \mathbb{Z}_{(p),+}^\times \lambda$ and $a_* [\eta]^p = [\eta']^p$. This shows the injectivity.

We show the surjectivity. Let $[\phi] \in G(\mathbb{Z}_{(p)}) \backslash G(\mathbb{A}_f^p) / U_N^p$ be a class, where $\phi \in G(\mathbb{A}_f^p)$. Let $\zeta := \nu(\phi) \in (\mathbb{A}_f^p)^\times$. Replacing ϕ by $a\phi$ for a suitable $a \in G(\mathbb{Q})$, we may assume that $\zeta \in (\hat{\mathbb{Z}}^{(p)})^\times$. Let $L := \phi(T^{(p)}(A)) \subset V^{(p)}(A)$ be the image of $T^{(p)}(A)$ under ϕ . By a theorem of Tate, there are an abelian variety A and a prime-to- p quasi-isogeny $\varphi : A \rightarrow A_0$ such that $\varphi : T^{(p)}(A) \simeq L \subset V^{(p)}(A)$. As φ is a prime-to- p quasi-isogeny, A is superspecial. Put $\lambda := \varphi^* \lambda_0$, considered as an element in $\text{Hom}(A, A^t) \otimes \mathbb{Z}_{(p)}$. We have an isomorphism $\eta := \varphi^{-1} \phi : (T^{(p)}(A_0), \langle \cdot, \cdot \rangle_{\lambda_0}) \simeq (T^{(p)}(A), \zeta \langle \cdot, \cdot \rangle_\lambda)$. This shows that λ is a principal polarization. Then we get an object $(A, \lambda, [\eta]^p)$ and this is sent to the class $[\phi]$ by the construction.

We check the compatibility with the Galois action. Let $\phi \in G(\mathbb{A}_f^p)$ and $\underline{A} = (A, \lambda, [\eta]^p) \in \Lambda_{g,N}^{(p)}$ be the element such that $\mathbf{c}_N^p(\underline{A}) = [\phi]$. Then there are an element $\varphi \in \text{G-isog}_{\mathbb{F}_p}^{(p)}(\underline{A}, \underline{A}_0)$ and an element $\eta \in [\eta]^p$ such that $\phi = \varphi \circ \eta$. Applying any element σ in \mathcal{G} , we get

$$\sigma(\phi) \in \text{G-isog}_{\mathbb{F}_p}^{(p)}(\sigma \underline{A}, \sigma \underline{A}_0), \quad \sigma(\eta) \in \text{GIsom}(V^{(p)}(\sigma \underline{A}_0), V^{(p)}(\sigma \underline{A})),$$

and $\sigma(\phi) = \sigma(\varphi) \circ \sigma(\eta)$. This yields $\mathbf{c}_N^p(\sigma \underline{A}) = [\sigma(\phi)]$. ■

Lemma 7.4. *Every member $(A, \lambda, \eta_N) \in \Lambda_{g,N}^*$ has a unique model (A', λ', η'_N) , up to isomorphism, over \mathbb{F}_{p^2} such that there is a prime-to- p quasi-isogeny $\varphi : A' \rightarrow A_0 \otimes \mathbb{F}_{p^2}$ such that $\varphi^* \lambda_0 \in \mathbb{Z}_{(p),+}^\times \cdot \lambda'$.*

PROOF. By Proposition 6.1, (A, λ) has a unique model (A', λ') over \mathbb{F}_{p^2} with the property. Since the relative Frobenius morphism $\pi_{A'/\mathbb{F}_{p^2}}$ is $-p$, the pull-back level structure η'_N is defined over \mathbb{F}_{p^2} . ■

Similarly to Proposition 6.1, we call the unique model over \mathbb{F}_{p^2} in Lemma 7.4 the *canonical model* over \mathbb{F}_{p^2} . We may identify the set $\Lambda_{g,N}^*$ with the set of isomorphism classes of superspecial g -dimensional principally polarized abelian varieties $\underline{A} = (A, \lambda, \eta_N)$ with level- N structure with respect to \underline{A}_0 such that the set $\text{G-isog}_{\mathbb{F}_{p^2}}^{(p)}(\underline{A}, \underline{A}_0)$ is non-empty.

For any prime-to- p positive integers $N|M$, we have a natural projection $\Lambda_{g,M}^* \rightarrow \Lambda_{g,N}^*$. Let

$$\tilde{\Lambda}_g^* := (\Lambda_{g,N}^*)_{p \nmid N}$$

be the tower of all superspecial loci with prime-to- p level structures. Elements of $\tilde{\Lambda}_g^*$ are represented as $(A, \lambda, \tilde{\eta})$, where (A, λ) is an element in Λ_g and $\tilde{\eta} \in \text{GIsom}(T^{(p)}(\underline{A}_0), T^{(p)}(\underline{A}))$ is a trivialization. It follows from Theorem 7.3 that the tower $\tilde{\Lambda}_g^*$ admits a right action of $G(\mathbb{A}_f^p)$ and we have a natural isomorphism

$$(7.4) \quad \mathbf{d}^p : G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / G(\mathbb{Z}_p) \simeq \tilde{\Lambda}_g^*$$

of pointed profinite sets which is compatible with the actions of $\text{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ from the left, and of $G(\mathbb{A}_f^p)$ from the right.

7.3. The Hecke operator $R(\pi_0)$ and type number. We define the operator $R(\pi_0)$ and the type number with level structure, which are almost identical with those in Section 1.

Let $M_0(U_N)$ the vector space of functions $f : G(\mathbb{A}_f) \rightarrow \mathbb{C}$ satisfying $f(axu) = f(x)$ for all $a \in G(\mathbb{Q})$ and $u \in U_N$. Let $\mathcal{H}(G, U_N)$ be the Hecke algebra of bi- U_N -invariant functions, which acts on the space $M_0(U_N)$ in the same way as (1.4) but the Haar measure takes volume one on U_N . Let $R(\pi_0)$ be the operator corresponding to the double coset $U_N(\pi_0) := U_N\pi_0 = \pi_0U_N$.

Let \mathcal{T}_N be the double coset space

$$\mathcal{T}_N := G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / \mathfrak{N}_N,$$

where \mathfrak{N}_N is the (open) subgroup of $G(\mathbb{A}_f)$ consisting of elements x such that

- (1) $\text{Int}(x)(\text{End}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes \hat{\mathbb{Z}}) = \text{End}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes \hat{\mathbb{Z}}$, and
- (2) the induced map

$$\text{Int}(x) : \text{End}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes (\mathbb{Z}/N\mathbb{Z}) \rightarrow \text{End}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes (\mathbb{Z}/N\mathbb{Z})$$

is the identity map.

It is not hard to show (see Lemma 6.6) that

$$(7.5) \quad \mathfrak{N}_N = D(\mathbb{Q}_p)G(\mathbb{Z}_p) \times Z(\mathbb{A}_f^p)U_N^p.$$

We call the cardinality T_N of \mathcal{T}_N the type number of the group G with level group U_N .

Let $\Lambda_{g,N}^*(\mathbb{F}_p) \subset \Lambda_{g,N}^*$ denote the subset consisting of objects (A, λ, η_N) whose isomorphism classes are defined over \mathbb{F}_p . In other words, $\Lambda_{g,N}^*(\mathbb{F}_p)$ is the subset of fixed points of the Frobenius map σ_p .

Theorem 7.5.

- (1) Every member $(A, \lambda, \eta_N) \in \Lambda_{g,N}^*(\mathbb{F}_p)$ has a model (A', λ', η'_N) defined over \mathbb{F}_p . Moreover, if $N \geq 3$, then the model (A', λ', η'_N) is unique up to isomorphism over \mathbb{F}_p and the base change $(A', \lambda', \eta'_N) \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$ is the canonical model over \mathbb{F}_{p^2} in $[(A, \lambda, \eta_N)]$ in the sense of Lemma 7.4.
- (2) Let (A, λ, η_N) be an object in $\Lambda_{g,N}^*$ and let $[x] \in G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / U_N$ be the class corresponding to the isomorphism class $[(A, \lambda, \eta_N)]$. Then $[(A, \lambda, \eta_N)]$ lies in $\Lambda_{g,N}^*(\mathbb{F}_p)$ if and only if

$$(7.6) \quad G(\mathbb{Q}) \cap xU_N(\pi_0)x^{-1} \neq \emptyset.$$

- (3) We have $\text{tr } R(\pi_0) = |\Lambda_{g,N}^*(\mathbb{F}_p)|$.
- (4) The natural map $\text{pr} : \Lambda_{g,N}^* \rightarrow \mathcal{T}_N$ induces a bijection between the set of orbits of $\Lambda_{g,N}^*$ under the action of $\text{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ with the set \mathcal{T}_N .
- (5) We have

$$\text{tr } R(\pi_0) = 2T_N - H_N,$$

where $H_N := |\Lambda_{g,N}^*|$ is the class number of G with level group U_N .

PROOF. (1) We may assume that $N \geq 2$ as the case $N = 1$ is treated in Section 6. By Lemma 7.4, we may assume that (A, λ, η_N) is the canonical model over \mathbb{F}_{p^2} in its isomorphism class. Then its conjugation $({}^{\sigma_p}A, {}^{\sigma_p}\lambda, {}^{\sigma_p}\eta_N)$ is also a canonical model over \mathbb{F}_{p^2} in its isomorphism class. By assumption, there is an isomorphism $a_{\sigma_p} : (A, \lambda, \eta_N) \simeq ({}^{\sigma_p}A, {}^{\sigma_p}\lambda, {}^{\sigma_p}\eta_N)$ over \mathbb{F}_{p^2} , as they are canonical models over \mathbb{F}_{p^2} in the same isomorphism class. Then $\sigma_p(a_{\sigma_p})a_{\sigma_p}$ is an automorphism of (A, λ, η)

and is equal to ± 1 ($= 1$ if $N \geq 3$). Using the same argument as in Proposition 6.3, we define recursively $a_{\sigma_p^i} := \sigma_p(a_{\sigma_p^{i-1}})$ and show that the map $\sigma \mapsto a_\sigma$ satisfies the 1-cocycle condition for the field extension $\mathbb{F}_{p^4}/\mathbb{F}_p$ (for $\mathbb{F}_{p^2}/\mathbb{F}_p$ if $N \geq 3$). Then by Weil's theorem, there are a model (A', λ', η'_N) over \mathbb{F}_p and an isomorphism $b : (A', \lambda', \eta'_N) \simeq (A', \lambda', \eta'_N)$ over \mathbb{F}_{p^4} (over \mathbb{F}_{p^2} if $N \geq 3$) such that $a_{\sigma_p} = \sigma_p(b) \circ b^{-1}$. When $N \geq 3$, we have shown that this model is compatible with the canonical model over \mathbb{F}_{p^2} . The uniqueness follows from a theorem of Serre (cf. [21, Lemma p. 207]) that the automorphism group $\text{Aut}(A, \lambda, \eta_N)$ is trivial.

The proofs for the statements (2), (3), (4) and (5) are the same as before. ■

Remark 7.6.

- (1) Similarly to Remark 6.10, we discuss a bit about models over \mathbb{F}_p . Let $\Lambda_{g,N}^{*,\text{nc}}(\mathbb{F}_p) \subset \Lambda_{g,N}^*(\mathbb{F}_p)$ denote the subset consisting of isomorphism classes in which a model \underline{A}' over \mathbb{F}_p exists such that the base change $\underline{A}' \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$ is the canonical model over \mathbb{F}_{p^2} in the sense of Lemma 7.4. We have $\Lambda_{g,N}^{*,\text{nc}}(\mathbb{F}_p) \subset \Lambda_{g,N}^*(\mathbb{F}_p)$ and $\Lambda_{g,N}^{*,\text{nc}}(\mathbb{F}_p) = \Lambda_{g,N}^*(\mathbb{F}_p)$ if $N \geq 3$. We do not know whether this equality holds when $N \leq 2$.
- (2) For $N \geq 3$, we have the following explicit formula (cf. Section 1)

$$(7.7) \quad H_N = |\text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})| \frac{(-1)^{g(g+1)/2}}{2^g} \left\{ \prod_{k=1}^g \zeta(1-2k) \right\} \cdot \prod_{k=1}^g \{p^k + (-1)^k\}.$$

7.4. Proof of Theorem 1.5. Now we describe the Galois action on the superspecial locus with the standard level- N structure. Let (\mathbb{Z}^{2g}, ψ) be the standard symplectic \mathbb{Z} -module of rank $2g$, and let GSp_{2g} be the group of symplectic similitudes defined over \mathbb{Z} . Let N be a prime-to- p positive integer as before. Let $\mathcal{A}_{g,1,N}$ denote the moduli space over $\text{Spec } \mathbb{Z}[1/N]$ of g -dimensional principally polarized abelian varieties (A, λ, α) with a (full) symplectic level- N structure. Recall that a full symplectic level- N structure on a g -dimensional principally polarized abelian scheme (A, λ) over a connected $\mathbb{Z}[1/N]$ -scheme S is an isomorphism $\alpha : (\mathbb{Z}/N\mathbb{Z})^{2g} \simeq A[N](S)$ such that there is an element $\zeta \in \mu_N(S)$ such that

$$(7.8) \quad e_\lambda(\alpha(x), \alpha(y)) = \zeta \psi(x, y), \quad \forall x, y \in (\mathbb{Z}/N\mathbb{Z})^{2g}.$$

We denote by $\Lambda_{g,N} \subset \mathcal{A}_{g,1,N}(\overline{\mathbb{F}}_p)$ the superspecial locus.

Put

$$(7.9) \quad H_f^p := \text{GIsom}(((\mathbb{A}_f^p)^{2g}, \psi), V^{(p)}(\underline{A}_0)).$$

The set H_f^p is a $(G(\mathbb{A}_f^p), \text{GSp}_{2g}(\mathbb{A}_f^p))$ -bi-torsor together with an action of the Galois group $\mathcal{G} = \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ from the left. The action of \mathcal{G} on $T^{(p)}(A_0)$ gives rise to a Galois representation

$$\rho : \mathcal{G} \rightarrow G(\hat{\mathbb{Z}}^{(p)}).$$

Using Proposition 4.3 (3), the action of \mathcal{G} on H_f^p is given as follows:

$$(7.10) \quad \sigma \cdot f = \rho(\sigma) \circ f, \quad \forall \sigma \in \mathcal{G}, f \in H_f^p.$$

Let

$$\tilde{\mathcal{A}}_g^{(p)} := (\mathcal{A}_{g,1,N})_{p \nmid N}$$

denote the tower of Siegel modular varieties with prime-to- p level structures over $\text{Spec } \mathbb{Z}_{(p)}$. Let $\tilde{\Lambda}_g \subset \tilde{\mathcal{A}}_g^{(p)}(\overline{\mathbb{F}}_p)$ be the superspecial locus. Elements in $\tilde{\Lambda}_g$ are represented as $(A, \lambda, \tilde{\alpha})$, where (A, λ) is an element in Λ_g and

$$\tilde{\alpha} \in \text{GIsom}((\hat{\mathbb{Z}}^{(p)})^{2g}, \psi), T^{(p)}(\underline{A})$$

is a trivialization. Suppose $(A, \lambda, \tilde{\alpha}) \in \tilde{\Lambda}_g$ is an object. We can choose an quasi-isogeny $\varphi \in \text{G-isog}_{\mathbb{F}_p}^{(p)}(\underline{A}, \underline{A}_0)$. The composition $\varphi \circ \tilde{\alpha}$

$$(\mathbb{A}_f^p)^{2g} \xrightarrow{\tilde{\alpha}} V^{(p)}(A) \xrightarrow{\varphi} V^{(p)}(A_0)$$

defines a well-defined map

$$\mathbf{b}^p : \tilde{\Lambda}_g \rightarrow G(\mathbb{Z}_{(p)}) \backslash H_f^p$$

which is compatible with the $\text{GSp}_{2g}(\mathbb{A}_f^p)$ -action. Using the same argument in the proof of Theorem 7.3, one shows that the map \mathbf{b}^p is bijective and \mathcal{G} -equivariant.

If we fix a trivialization

$$\tilde{\alpha}_0 \in \text{GIsom}((\hat{\mathbb{Z}}^{(p)})^{2g}, \psi), T^{(p)}(\underline{A}_0),$$

then we get

- a Galois representation

$$\rho_0 : \mathcal{G} \rightarrow \text{GSp}_{2g}(\hat{\mathbb{Z}}^{(p)})$$

such that the following diagram

$$(7.11) \quad \begin{array}{ccc} (\hat{\mathbb{Z}}^{(p)})^{2g} & \xrightarrow{\tilde{\alpha}_0} & T^{(p)}(A_0) \\ \downarrow \rho_0(\sigma) & & \downarrow \rho(\sigma) \\ (\hat{\mathbb{Z}}^{(p)})^{2g} & \xrightarrow{\tilde{\alpha}_0} & T^{(p)}(A_0), \end{array}$$

commutes,

- an isomorphism

$$(7.12) \quad j_0 : \text{GSp}_{2g}(\mathbb{A}_f^p) \longrightarrow H_f^p, \quad \phi' \mapsto \tilde{\alpha}_0 \circ \phi',$$

and

- an isomorphism

$$(7.13) \quad i_0 : G(\mathbb{A}_f^p) \longrightarrow \text{GSp}_{2g}(\mathbb{A}_f^p), \quad \phi \mapsto \tilde{\alpha}_0^{-1} \circ \phi \circ \tilde{\alpha}_0.$$

Let \mathcal{G} act on $\text{GSp}_{2g}(\mathbb{A}_f^p)$ by the action ρ_0 :

$$(7.14) \quad \sigma \cdot \phi' := \rho_0(\sigma)\phi', \quad \forall \sigma \in \mathcal{G}, \phi' \in \text{GSp}_{2g}(\mathbb{A}_f^p).$$

One checks that

$$\sigma \cdot j_0(\phi') = \sigma \cdot \tilde{\alpha}_0 \circ \phi' = \rho(\sigma) \circ \tilde{\alpha}_0 \circ \phi' = \tilde{\alpha}_0 \circ \rho_0(\sigma)\phi'.$$

That is, the following diagram

$$\begin{array}{ccc} \text{GSp}_{2g}(\mathbb{A}_f^p) & \xrightarrow{j_0} & H_f^p \\ \downarrow \sigma & & \downarrow \sigma \\ \text{GSp}_{2g}(\mathbb{A}_f^p) & \xrightarrow{j_0} & H_f^p \end{array}$$

commutes. Therefore, we obtain an isomorphism (depending on the choice of $\tilde{\alpha}_0$)

$$(7.15) \quad \mathbf{b}_0^p : \tilde{\Lambda}_g \simeq i_0(G(\mathbb{Z}_{(p)})) \backslash \mathrm{GSp}_{2g}(\mathbb{A}_f^p)$$

which is compatible with the $\mathrm{GSp}_{2g}(\mathbb{A}_f^p)$ -action and the \mathcal{G} -action in (7.14). This completes the proof of Theorem 1.5.

8. THE NON-PRINCIPAL GENUS CASE

In previous sections we investigate arithmetic properties of *principally polarized* superspecial abelian varieties, as well as the relationship to the trace of certain Hecke operator on the space of automorphic forms of weight zero. These abelian varieties correspond to the principal genus of the group G . Since the non-principal genus case is of equal importance (see Section 8.1), we include the analogous results for these superspecial abelian varieties as well. The proofs of most results are the same as the principal genus case and are omitted.

8.1. The class numbers $H_n(p, 1)$ and $H_n(1, p)$. We start with the arithmetic aspect of polarized superspecial abelian varieties which are related to components of the supersingular locus of $\mathcal{A}_g \otimes \overline{\mathbb{F}}_p$, the coarse moduli space over $\overline{\mathbb{F}}_p$ of g -dimensional principally polarized abelian varieties. Our references are Ibukiyama-Katsura-Oort [11, Section 2] and Li-Oort [19, Section 4].

Let B be the quaternion algebra over \mathbb{Q} ramified exactly at $\{p, \infty\}$, and let \mathcal{O} be a maximal order of B . Put $V = B^{\oplus n}$, regarded as a left B -module of row vectors, and let $\psi(x, y) = \sum_{i=1}^n x_i \bar{y}_i$ be the standard Hermitian form on V , where the map $y_i \mapsto \bar{y}_i$ is the canonical involution on B . Let G be the algebraic group of ψ -similitudes over \mathbb{Q} ; the group of \mathbb{Q} -points of G is

$$G(\mathbb{Q}) := \{h \in M_n(B) \mid h \bar{h}^t = r I_n \text{ for some } r \in \mathbb{Q}^\times\}.$$

(Note that the group G here is isomorphic to the generic fiber $G_{\mathbb{Q}}$ of the group scheme G over $\mathrm{Spec} \mathbb{Z}$ defined in Introduction when $n = g$. Thus, we use the same notation.)

Two \mathcal{O} -lattices L and L' in $B^{\oplus n}$ are called *globally equivalent* (denoted by $L \sim L'$) if $L' = Lh$ for some element $h \in G(\mathbb{Q})$. For any finite place v of \mathbb{Q} , we write $B_v := B \otimes \mathbb{Q}_v$, $\mathcal{O}_v := \mathcal{O} \otimes \mathbb{Z}_v$ and $L_v := L \otimes \mathbb{Z}_v$. Two \mathcal{O} -lattices L and L' in $B^{\oplus n}$ are called *locally equivalent at v* (denoted by $L_v \sim L'_v$) if $L'_v = L_v h_v$ for some element $h_v \in G(\mathbb{Q}_v)$. A *genus* of \mathcal{O} -lattices is a maximal set of (global) \mathcal{O} -lattices in $B^{\oplus n}$ which are equivalent to each other locally at every finite place v .

We define an \mathcal{O}_p -lattice $N_p \subset B_p^{\oplus n}$ as follows:

$$N_p := \mathcal{O}_p^{\oplus n} \cdot \begin{pmatrix} I_r & 0 \\ 0 & \pi I_{n-r} \end{pmatrix} \cdot \xi \subset B_p^{\oplus n},$$

where r is the integer $[n/2]$, π is a uniformizer in \mathcal{O}_p , and ξ is an element in $\mathrm{GL}_n(B_p)$ such that

$$\xi \bar{\xi}^t = \text{anti-diag}(1, 1, \dots, 1).$$

Definition 8.1.

(1) Let $\mathcal{L}_n(p, 1)$ denote the set of \mathcal{O} -lattices L in $B^{\oplus n}$ such that $L_v \sim \mathcal{O}_v^{\oplus n}$ at every finite place v . The set $\mathcal{L}_n(p, 1)$ is called the *principal genus*. Let $\mathcal{L}_n(p, 1)/\sim$ denote the set of global equivalence classes in $\mathcal{L}_n(p, 1)$. As a well-known fact,

$\mathcal{L}_n(p, 1)/\sim$ is a finite set. The cardinality $H_n(p, 1) := \#\mathcal{L}_n(p, 1)/\sim$ is called the *class number* of the principal genus.

(2) Let $\mathcal{L}_n(1, p)$ denote the set of \mathcal{O} -lattices L in $B^{\oplus n}$ such that $L_p \sim N_p$ and $L_v \sim \mathcal{O}_v^{\oplus n}$ at every finite place $v \neq p$. The set $\mathcal{L}_n(1, p)$ is called the *non-principal genus*. Let $\mathcal{L}_n(1, p)/\sim$ denote the set of global equivalence classes in $\mathcal{L}_n(1, p)$. We know that $\mathcal{L}_n(1, p)/\sim$ is a finite set. The cardinality $H_n(1, p) := \#\mathcal{L}_n(1, p)/\sim$ is called the *class number* of the non-principal genus.

Recall that Λ_g is the set of isomorphism classes of g -dimensional principally polarized superspecial abelian varieties over $\overline{\mathbb{F}}_p$. When $g = 2d > 0$ is even, we denote by $\Sigma_g = \Sigma_g(\overline{\mathbb{F}}_p)$ the set of isomorphism classes of g -dimensional polarized superspecial abelian varieties (A, λ) of degree p^{2d} over $\overline{\mathbb{F}}_p$ satisfying $\ker \lambda = A[F]$. Here F is the relative Frobenius morphism $A \rightarrow A^{(p)}$ over $\overline{\mathbb{F}}_p$.

Let \mathcal{S}_g denote the supersingular locus of the Siegel moduli space $\mathcal{A}_g \otimes \overline{\mathbb{F}}_p$; it is a closed reduced subscheme of finite type over $\overline{\mathbb{F}}_p$. Let $\Pi_0(\mathcal{S}_g)$ denote the set of irreducible components of \mathcal{S}_g .

Theorem 8.2 (Li-Oort [19]). *We have*

$$|\Pi_0(\mathcal{S}_g)| = \begin{cases} |\Lambda_g| & \text{if } g \text{ is odd;} \\ |\Sigma_g| & \text{if } g = 2d \text{ is even.} \end{cases}$$

The arithmetic part for the supersingular locus \mathcal{S}_g is given by the following proposition.

Proposition 8.3.

- (1) *For any positive integer g , one has $|\Lambda_g| = H_g(p, 1)$.*
- (2) *For any even positive integer $g = 2d$, one has $|\Sigma_g| = H_g(1, p)$.*

PROOF. (1) See [11, Theorem 2.10]. (2) See [19, Proposition 4.7].

8.2. From on now in this section, let $g = 2d$ be an even positive integer. Suppose that there is a g -dimensional superspecial polarized abelian variety $\underline{A}'_0 = (A'_0, \lambda'_0)$ over $\overline{\mathbb{F}}_p$ such that the polarization degree is p^{2d} , $\ker \lambda'_0 = A'_0[F]$ and $(\pi'_0)^2 = -p$, where π'_0 is the Frobenius endomorphism of A'_0 . The existence of such an object may depend on p and g ; for example it exists if $\left(\frac{-1}{p}\right) = 1$ or $4|g$. Nevertheless we fix one when it exists. Let $G'_1 \subset G'$ be the automorphism group schemes over $\text{Spec } \mathbb{Z}$ associated to the object (A'_0, λ'_0) , defined similarly as in Section 5.1. Let N be a positive *prime-to- p* integer, and let U'_N be the kernel of the reduction map $G'(\hat{\mathbb{Z}}) \rightarrow G'(\mathbb{Z}/N\mathbb{Z})$. The generic fiber $G'_\mathbb{Q}$ of G' is isomorphic to $G_\mathbb{Q}$, so we can also consider U'_N as an open compact subgroup of $G(\mathbb{A}_f)$.

Denote by $\Sigma_{g,N}^* = \Sigma_{g,N}^*(\overline{\mathbb{F}}_p)$ the set of isomorphism classes of objects (A, λ, η_N) over $\overline{\mathbb{F}}_p$, where (A, λ) is an object in Σ_g and η_N is a level- N structure on (A, λ) with respect to \underline{A}'_0 (defined in the same way as in Section 7.1). Two objects (A, λ, η_N) and (A', λ', η'_N) in $\Sigma_{g,N}^*$ are isomorphic, denoted by $(A, \lambda, \eta_N) \simeq (A', \lambda', \eta'_N)$, if there is an isomorphism $\varphi : A \rightarrow A'$ such that $\varphi^* \lambda' = \lambda$ and $\varphi_* \eta_N = \eta'_N$.

As in the proof of Lemma 7.1, each level- N structure η_N on (A, λ) with respect to \underline{A}'_0 uniquely determines a U'_N -orbit

$$[\eta] := \{\eta \in \prod_{\ell} \text{GIsom}(\underline{A}'_0(\ell), \underline{A}(\ell)) \mid \eta|_{A'_0[N]} = \eta_N\}$$

in the $G'(\hat{\mathbb{Z}})$ -torsor $\prod_{\ell} \text{GIsom}(\underline{A}'_0(\ell), \underline{A}(\ell))$.

The Galois group $\mathcal{G} = \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ acts naturally on the topological group $G'(\mathbb{A}_f)$ and this action is given by (cf. Theorem 1.1)

$$(8.1) \quad \sigma_p(x_{\ell})_{\ell} = (\pi'_0 x_{\ell} \pi_0'^{-1})_{\ell}, \quad (x_{\ell})_{\ell} \in G'(\mathbb{A}_f).$$

Theorem 8.4. *There is a natural \mathcal{G} -equivariant bijective map*

$$\mathbf{c}'_N : \Sigma_{g,N}^* \rightarrow G'(\mathbb{Q}) \backslash G'(\mathbb{A}_f) / U'_N$$

for which the base point $(A'_0, \lambda'_0, \text{id})$ is sent to the identity class [1].

PROOF. This is the analogue of Theorem 7.3. The proof is the same and is omitted. ■

Lemma 8.5. *Every member $(A, \lambda, \eta_N) \in \Sigma_{g,N}^*$ has a unique model (A', λ', η'_N) , up to isomorphism, over \mathbb{F}_{p^2} such that there is a prime-to- p quasi-isogeny $\varphi : A' \rightarrow A'_0 \otimes \mathbb{F}_{p^2}$ such that $\varphi^* \lambda'_0 \in \mathbb{Z}_{(p),+}^{\times} \cdot \lambda'$.*

PROOF. This is the analogue of Lemma 7.4. The proof is the same and is omitted. ■

For any two prime-to- p positive integers M and N with $N|M$, we have a natural projection $\Sigma_{g,M}^* \rightarrow \Sigma_{g,N}^*$. Let

$$\tilde{\Sigma}_g^* := (\Sigma_{g,N}^*)_{p \nmid N}$$

be the tower. Elements of $\tilde{\Sigma}_g^*$ are represented as $(A, \lambda, \tilde{\eta})$, where (A, λ) is an element in Σ_g and $\tilde{\eta} \in \text{GIsom}(T^{(p)}(\underline{A}'_0), T^{(p)}(\underline{A}))$ is a trivialization. It follows from Theorem 8.4 that the tower $\tilde{\Sigma}_g^*$ admits a right action of $G'(\mathbb{A}_f^p)$ and we have a natural isomorphism

$$(8.2) \quad \mathbf{d}'^p : G'(\mathbb{Q}) \backslash G'(\mathbb{A}_f) / G'(\mathbb{Z}_p) \simeq \tilde{\Sigma}_g^*$$

of pointed profinite sets which is compatible with the actions of $\text{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ from the left, and of $G'(\mathbb{A}_f^p)$ from the right.

8.3. The Hecke operator $R(\pi'_0)$ and type number. We define the operator $R(\pi'_0)$ and the type number with level structure, which are almost identical with those in Section 7.3.

Let $M_0(U'_N)$ the vector space of functions $f : G'(\mathbb{A}_f) \rightarrow \mathbb{C}$ satisfying $f(axu) = f(x)$ for all $a \in G'(\mathbb{Q})$ and $u \in U'_N$. The Hecke algebra $\mathcal{H}(G', U'_N)$ acts on the space $M_0(U_N)$ in the same way as in (1.4) where the Haar measure takes volume one on the open compact subgroup U'_N . Let $R(\pi'_0)$ be the operator corresponding to the double coset $U'_N(\pi'_0) := U'_N \pi'_0 = \pi'_0 U'_N$.

Let \mathcal{T}'_N be the double coset space

$$\mathcal{T}'_N := G'(\mathbb{Q}) \backslash G'(\mathbb{A}_f) / \mathfrak{N}'_N,$$

where \mathfrak{N}'_N is the (open) subgroup of $G'(\mathbb{A}_f)$ consisting of elements x such that

- (1) $\text{Int}(x)(\text{End}(A'_0 \otimes \overline{\mathbb{F}}_p) \otimes \hat{\mathbb{Z}}) = \text{End}(A'_0 \otimes \overline{\mathbb{F}}_p) \otimes \hat{\mathbb{Z}}$, and
- (2) the induced map

$$\text{Int}(x) : \text{End}(A'_0 \otimes \overline{\mathbb{F}}_p) \otimes (\mathbb{Z}/N\mathbb{Z}) \rightarrow \text{End}(A'_0 \otimes \overline{\mathbb{F}}_p) \otimes (\mathbb{Z}/N\mathbb{Z})$$

is the identity map.

It is not hard to show (see Lemma 6.6) that

$$(8.3) \quad \mathfrak{N}'_N = D(\mathbb{Q}_p)G'(\mathbb{Z}_p) \times Z(\mathbb{A}_f^p)U'^p_N,$$

where $U'^p_N \subset G'(\mathbb{A}_f^p)$ is the prime-to- p component of the open compact subgroup U'_N . The cardinality $T'_N := |\mathcal{T}'_N|$ is called the type number of the group G' with level group U'_N .

Let $\Sigma_{g,N}^*(\mathbb{F}_p) \subset \Sigma_{g,N}^*$ be the subset of fixed points of the Frobenius map σ_p .

Theorem 8.6.

- (1) Every member $(A, \lambda, \eta_N) \in \Sigma_{g,N}^*(\mathbb{F}_p)$ has a model (A', λ', η'_N) defined over \mathbb{F}_p . Moreover, if $N \geq 3$, then the model (A', λ', η'_N) is unique up to isomorphism over \mathbb{F}_p and the base change $(A', \lambda', \eta'_N) \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$ is the canonical model over \mathbb{F}_{p^2} in $[(A, \lambda, \eta_N)]$ in the sense of Lemma 8.5.
- (2) Let (A, λ, η_N) be an object in $\Sigma_{g,N}^*$ and let $[x] \in G'(\mathbb{Q}) \backslash G'(\mathbb{A}_f) / U'_N$ be the class corresponding to the isomorphism class $[(A, \lambda, \eta_N)]$. Then the class $[(A, \lambda, \eta_N)]$ lies in $\Sigma_{g,N}^*(\mathbb{F}_p)$ if and only if

$$(8.4) \quad G'(\mathbb{Q}) \cap xU'_N(\pi'_0)x^{-1} \neq \emptyset.$$

- (3) We have $\text{tr } R(\pi'_0) = |\Sigma_{g,N}^*(\mathbb{F}_p)|$.
- (4) The natural map $\text{pr} : \Sigma_{g,N}^* \rightarrow \mathcal{T}'_N$ induces a bijection between the set of orbits of $\Sigma_{g,N}^*$ under the action of $\text{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ with the set \mathcal{T}'_N .
- (5) We have

$$(8.5) \quad \text{tr } R(\pi'_0) = 2T'_N - H'_N,$$

where $H'_N = |\Sigma_{g,N}^*|$ is the class number of G' with level group U'_N .

PROOF. This is the analogue of Theorem 7.5. The proof is the same and is omitted. ■

For $N \geq 3$, we have the following explicit formula (see [36, Theorem 6.6]; note that in loc. cit. one fixes a choice of a primitive N th root of unity ζ_N .)

$$(8.6) \quad H'_N = |\text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})| \frac{(-1)^{g(g+1)/2}}{2^g} \left\{ \prod_{k=1}^g \zeta(1-2k) \right\} \cdot \prod_{k=1}^d (p^{4k-2} - 1).$$

9. TRACE FORMULA FOR GROUPS OF COMPACT TYPE

The goal of this section is to calculate the trace of the Hecke operator $R(\pi_0)$ (or $R(\pi'_0)$) for the groups G (or G') arising from the previous sections using the Selberg trace formula. Since one has the explicit formula for the class number H_N or H'_N (see (7.7) and (8.6)), by Theorems 7.5 and 8.6, we obtain a formula for the type numbers T_N or T'_N . For other possible applications, we work on slightly more general groups and study the trace of specific Hecke operators. This section is independent from the previous sections; some notations are different.

9.1. Groups. Let G be a smooth group scheme over $\text{Spec } \mathbb{Z}$ satisfying the property: The generic fiber $G_{\mathbb{Q}} := G \otimes_{\mathbb{Z}} \mathbb{Q}$ is a connected reductive group and the arithmetic subgroup $G(\mathbb{Q})$ is discrete in $G(\mathbb{A}_f)$. We know that $G(\mathbb{Q})$ is discrete in $G(\mathbb{A}_f)$ if and only the quotient space $G(\mathbb{Q}) \backslash G(\mathbb{A}_f)$ is compact. Moreover, we have the following equivalent statements; see [8, Proposition 1.4].

Proposition 9.1. *Let G be a connected reductive algebraic group over \mathbb{Q} . The following conditions are equivalent:*

- (1) *Every arithmetic subgroup Γ of $G(\mathbb{Q})$ is finite.*
- (2) *$\Gamma = \{e\}$ is an arithmetic subgroup of $G(\mathbb{Q})$.*
- (3) *$G(\mathbb{Q})$ is a discrete subgroup of the locally compact topological group $G(\mathbb{A}_f)$.*
- (4) *$G(\mathbb{Q})$ is a discrete subgroup of the locally compact topological group $G(\mathbb{A}_f)$, and the quotient space $G(\mathbb{Q}) \backslash G(\mathbb{A}_f)$ is compact.*
- (5) *The Lie group*

$$G(\mathbb{R})_1 := \{g \in G(\mathbb{R}) \mid |\chi(g)| = 1, \forall \text{ rational character } \chi : G \rightarrow \mathbb{G}_m\}$$

is a maximal compact subgroup of $G(\mathbb{R})$.

- (6) *The maximal \mathbb{Q} -split torus of the center $Z(G)$ of G gives rise to a maximal \mathbb{R} -split torus of $G_{\mathbb{R}}$.*
- (7) *For every irreducible rational representation V of G there is a character $\mu : G \rightarrow \mathbb{G}_m$ and a positive definite symmetric bilinear form $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{Q}$ which satisfy*

$$\langle gv, gv' \rangle = \mu(g) \langle v, v' \rangle$$

for all g in $G(\mathbb{Q})$ and v, v' in V .

9.2. Hecke operators $R(\pi)$. Denote by $L^2(G) = L^{2,\infty}(G(\mathbb{Q}) \backslash G(\mathbb{A}_f))$ the vector space of locally constant \mathbb{C} -valued functions on $G(\mathbb{Q}) \backslash G(\mathbb{A}_f)$, endowed with an inner product defined by

$$\langle f, g \rangle := \int_{G(\mathbb{Q}) \backslash G(\mathbb{A}_f)} f(x) \overline{g(x)} dx,$$

for a Haar measure dx on $G(\mathbb{A}_f)$ which we shall specify later. This is a pre-Hilbert space as the limit of locally constant functions need not to be locally constant. For example, the limit of the sequence of characteristic functions $\mathbf{1}_{G(\mathbb{Q})U_n}$ for a decreasing separated sequence of open compact subgroups U_n is the delta function $\delta_{[1]}$ supported on the identity class [1].

The group $G(\mathbb{A}_f)$ acts on the space $L^2(G)$ by right translation, denoted by R . Since the topological space $G(\mathbb{Q}) \backslash G(\mathbb{A}_f)$ is compact, every function f in $L^2(G)$ is invariant under an open subgroup $U \subset G(\mathbb{A}_f)$, that is, f is a smooth vector. Also for any open compact subgroup U , the invariant subspace

$$L^2(G)^U = L^{2,\infty}(G(\mathbb{Q}) \backslash G(\mathbb{A}_f)/U) = \mathcal{C}(G(\mathbb{Q}) \backslash G(\mathbb{A}_f)/U)$$

consisting of constant functions on the finite set $G(\mathbb{Q}) \backslash G(\mathbb{A}_f)/U$ is finite-dimensional. In other words, the representation $L^2(G)$ of $G(\mathbb{A}_f)$ is admissible. Denote by $\mathcal{H}(G)$ the Hecke algebra of \mathbb{C} -valued, locally constant, compactly supported functions on $G(\mathbb{A}_f)$; the multiplication is given by the convolution. The Hecke algebra $\mathcal{H}(G)$ acts on the space $L^2(G)$ as follows: For $\varphi \in \mathcal{H}(G)$, $f \in L^2(G)$,

$$R(\varphi)f(x) := \int_{G(\mathbb{A}_f)} \varphi(y) R(y)f(x) dx = \int_{G(\mathbb{A}_f)} \varphi(y) f(xy) dx.$$

For any positive integer N , one defines an open compact subgroup U_N as the kernel of the reduction map

$$\text{Red}_N : G(\hat{\mathbb{Z}}) \rightarrow G(\mathbb{Z}/N\mathbb{Z}).$$

Fix an element π of $G(\mathbb{Q})$ which normalizes U_N for all N . In many cases, any element in the normalizer \mathfrak{N} of the open compact subgroup $U_1 = G(\hat{\mathbb{Z}})$ satisfies this property. For example, this is the case if the \mathbb{Z} -structure of G is induced by a \mathbb{Z} -lattice for a rational faithful representation $\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}(V_{\mathbb{Q}})$ of $G_{\mathbb{Q}}$. Let $\varphi_{\pi,N}$ be the characteristic function of the double coset $U_N\pi U_N = \pi U_N = U_N\pi$ and we write $R_N(\pi) = R(\varphi_{\pi,N})$, where N is a positive integer. The goal is to calculate the trace of the Hecke operator $R_N(\pi)$. Here we normalize the Haar measure so that it takes volume one on the open compact subgroup U_N . The meaning of the trace $\mathrm{tr} R_N(\pi)$ can be interpreted as the number of fixed points in the double coset space $G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / U_N$ under the translation $[x] \mapsto [x\pi]$. Note that the translation is well-defined as π normalizes U_N . Indeed, the image of $R_N(\pi)$ is contained in the U_N -invariant subspace $\mathcal{C}(G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / U_N)$. So $\mathrm{tr} R_N(\pi)$ is equal to the trace of its restriction

$$R_N(\pi) : \mathcal{C}(G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / U_N) \rightarrow \mathcal{C}(G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / U_N).$$

This map is induced by the translation $[x] \mapsto [x\pi]$ and hence its trace is equal to the number of fixed points.

To simplify notation we shall write φ_{π} for $\varphi_{\pi,N}$ and $R(\pi)$ for $R_N(\pi)$, respectively, with understanding that these also depend on N .

9.3. Trace of $R(\pi)$. The standard argument in the trace formula (cf. [6]) shows that the operator $R(\pi)$ is of trace class and its trace can be calculated by the following integral

$$\mathrm{tr} R(\pi) = \int_{G(\mathbb{Q}) \backslash G(\mathbb{A}_f)} K_{\pi}(x, x) dx,$$

where

$$K_{\pi}(x, y) := \sum_{\gamma \in G(\mathbb{Q})} \varphi_{\pi}(x^{-1}\gamma y).$$

Note that when x and y vary in a fixed open compact subset, there are only finitely many non-zero terms in the sum of $K_{\pi}(x, y)$. Regrouping the terms in the standard way (cf. [6]), we get

$$(9.1) \quad \mathrm{tr} R(\pi) = \sum_{\gamma \in G(\mathbb{Q}) / \sim} a(G_{\gamma}) O_{\gamma}(\varphi_{\pi}),$$

where

- $G(\mathbb{Q}) / \sim$ denotes the set of conjugacy classes of $G(\mathbb{Q})$,
- G_{γ} denotes the centralizer of γ in G , and
- $a(G_{\gamma}) := \mathrm{vol}(G_{\gamma}(\mathbb{Q}) \backslash G_{\gamma}(\mathbb{A}_f))$, and

$$(9.2) \quad O_{\gamma}(\varphi_{\pi}) := \int_{G_{\gamma}(\mathbb{A}_f) \backslash G(\mathbb{A}_f)} \varphi_{\pi}(x^{-1}\gamma x) \frac{dx}{dx_{\gamma}},$$

where dx_{γ} is a Haar measure on $G_{\gamma}(\mathbb{A}_f)$.

Note that the whole term $a(G_{\gamma}) O_{\gamma}(\varphi_{\pi})$ does not depend on the choice of the Haar measure dx_{γ} . As the closed subgroup $G_{\gamma}(\mathbb{A}_f)$ is unimodular, the right $G(\mathbb{A}_f)$ -invariant Radon measure dx/dx_r is defined and it is characterized by the following property:

$$(9.3) \quad \int_{G(\mathbb{A}_f)} f dx = \int_{G_{\gamma}(\mathbb{A}_f) \backslash G(\mathbb{A}_f)} \int_{G_{\gamma}(\mathbb{A}_f)} f(x_{\gamma} x) dx_{\gamma} \frac{dx}{dx_{\gamma}}$$

for all functions $f \in C_c^\infty(G(\mathbb{A}_f))$. Using this formula, one easily shows

$$(9.4) \quad \text{vol}_{dx/dx_\gamma}(G_\gamma(\mathbb{A}_f) \backslash G_\gamma(\mathbb{A}_f)U) = \frac{\text{vol}_{dx}(U)}{\text{vol}_{dx_\gamma}(G_\gamma(\mathbb{A}_f) \cap U)}$$

for any open compact subgroup $U \subset G(\mathbb{A}_f)$, or more generally,

$$(9.5) \quad \text{vol}_{dx/dx_\gamma}(G_\gamma(\mathbb{A}_f) \backslash G_\gamma(\mathbb{A}_f)aU) = \frac{\text{vol}_{dx}(U)}{\text{vol}_{dx_\gamma}(G_\gamma(\mathbb{A}_f) \cap aUa^{-1})}$$

for any element $a \in G(\mathbb{A}_f)$. See Kottwitz [17, Section 2.4]. In our situation, any element $\gamma \in G(\mathbb{Q})$ is semi-simple. Therefore, any $G(\mathbb{A}_f)$ -conjugacy class is closed and the orbital integral $O_\gamma(\varphi_\pi)$ is a finite sum.

For elements x and γ in $G(\mathbb{Q})$ (resp. in $G(\mathbb{Q}_v)$ or $G(\mathbb{A}_f)$), we write $x \cdot \gamma = x^{-1}\gamma x$, the conjugation of γ by x . Put

$$(9.6) \quad \Delta_N := \{\gamma \in G(\mathbb{Q}) \mid G(\mathbb{A}_f) \cdot \gamma \cap \pi U_N \neq \emptyset\} / \sim_{G(\mathbb{Q})}.$$

We show that Δ_N is a finite set.

Let $C \subset G(\mathbb{A}_f)$ be an open compact subset such that $G(\mathbb{A}_f) = G(\mathbb{Q})C$. For example, if we write $G(\mathbb{A}_f)$ as a finite disjoint union of double coset:

$$G(\mathbb{A}_f) := \coprod_{i=1}^h G(\mathbb{Q})c_i U_1,$$

then take C to be the union of $c_i U_1$ for $i = 1, \dots, h$. Put

$$X_N := \bigcup_{c \in C} c^{-1} \cdot \pi U_N.$$

Since X_N is an image of the compact set $C \times \pi U_N$, it is compact. If γ is an element of $G(\mathbb{Q})$ which lies in $G(\mathbb{A}_f) \cdot \pi U_N$, then there is an element $a \in G(\mathbb{Q})$ such that $a \cdot \gamma \in X_N$. The element $a \cdot \gamma$ lies in the intersection $G(\mathbb{Q}) \cap X_N$, which is a finite set. Since Δ_N consists of elements γ as above modulo the $G(\mathbb{Q})$ -conjugation, the set Δ_N is finite.

For each class $\bar{\gamma} \in \Delta_N$, we select a representative γ in $X_N \cap G(\mathbb{Q})$ and choose the Haar measure dx_γ so that

$$(9.7) \quad \text{vol}(U_{\gamma,N}) = 1, \quad \text{where } U_{\gamma,N} := G_\gamma(\mathbb{A}_f) \cap U_N.$$

Put

$$\mathcal{E}_\gamma := \{x \in G(\mathbb{A}_f) \mid x^{-1}\gamma x \in \pi U_N\},$$

which is the support of the function $\phi_\gamma(x) := \varphi_\pi(x^{-1}\gamma x)$. It is clear that \mathcal{E}_γ is stable under the left $G_\gamma(\mathbb{A}_f)$ -action and the right U_N -action. By our choice of Haar measures on $G(\mathbb{A}_f)$ and $G_\gamma(\mathbb{A}_f)$, the orbital integral $O_\gamma(\varphi_\pi)$ can be calculated using the formula (see (9.5))

$$O_\gamma(\varphi_\pi) = \sum_{[a] \in G_\gamma(\mathbb{A}_f) \backslash \mathcal{E}_\gamma / U_N} \text{vol}(G_\gamma(\mathbb{A}_f) \cap aUa^{-1})^{-1}.$$

We have shown the following result.

Proposition 9.2. *Let $\Delta_N \subset G(\mathbb{Q})/\sim$ be the subset of $G(\mathbb{Q})$ -conjugacy classes defined in (9.6).*

- (1) *The set Δ_N is finite.*

(2) *We have*

$$(9.8) \quad \mathrm{tr} R(\pi) = \sum_{\bar{\gamma} \in \Delta_N} a(G_\gamma) O_\gamma(\varphi_\pi)$$

and

$$(9.9) \quad O_\gamma(\varphi_\pi) = \sum_{[a] \in G_\gamma(\mathbb{A}_f) \backslash \mathcal{E}_\gamma / U_N} \mathrm{vol}(G_\gamma(\mathbb{A}_f) \cap aUa^{-1})^{-1}.$$

9.4. Trace of $R(\pi)$ when U_N small. Put

$$\Delta_f(\pi) := \{\gamma \in G(\mathbb{Q}) \mid \gamma \in G(\mathbb{A}_f) \cdot \pi\} / \sim_{G(\mathbb{Q})}.$$

Clearly we have $\Delta_f(\pi) \subset \Delta_N$.

Lemma 9.3. *There is a positive integer N_0 such that for all positive integers N divisible by N_0 , we have $\Delta_N = \Delta_f(\pi)$.*

PROOF. Since $G(\mathbb{Q}) \cap X_N$ is finite, there is a positive integer N_0 such that $G(\mathbb{Q}) \cap X_N$ remains the same for all N with $N_0 \mid N$. Let γ be an element in $G(\mathbb{Q}) \cap X_N$. Then for all n with $N_0 \mid n$, we have $\gamma = c_n \pi u_n c_n^{-1}$ for some $c_n \in C$ and $u_n \in U_n$. Since C is compact, there is a subsequence $\{c_{m_i}\}$ of $\{c_n\}$ which converges to an element $c_0 \in C$. As $i \rightarrow \infty$, we get $\gamma = c_0 \pi c_0^{-1}$. This shows the lemma. \blacksquare

Suppose an element $\gamma \in G(\mathbb{Q})$ has the form $y^{-1} \pi y$ for some $y \in G(\mathbb{A}_f)$. We show that the term $a(G_\gamma) O_\gamma(\varphi_\pi)$ in (9.8) is equal to $a(G_\pi) O_\pi(\varphi_\pi)$. First, it is easy to show that an element $x \in G(\mathbb{Q})$ lies in $G_\gamma(\mathbb{Q})$ if and only if $xyx^{-1} \in G_\pi(\mathbb{Q})$; thus $yG_\gamma(\mathbb{Q})y^{-1} = G_\pi(\mathbb{Q})$. Let $t = yx$. The map $x \mapsto t$ induces an homeomorphism

$$G_\gamma(\mathbb{Q}) \backslash G(\mathbb{A}_f) \simeq G_\pi(\mathbb{Q}) \backslash G(\mathbb{A}_f).$$

We have

$$(9.10) \quad \begin{aligned} a(G_\gamma) O_\gamma(\varphi_\pi) &= \int_{G_\gamma(\mathbb{Q}) \backslash G(\mathbb{A}_f)} \varphi_\pi(x^{-1} y^{-1} \pi y x) dx \\ &= \int_{G_\pi(\mathbb{Q}) \backslash G(\mathbb{A}_f)} \varphi_\pi(t^{-1} \pi t) dt = a(G_\pi) O_\pi(\varphi_\pi). \end{aligned}$$

Lemma 9.3 and the equality (9.10) show that when U_N is small, the trace of the Hecke operator $R(\pi)$ can be simplified significantly.

Theorem 9.4. *There is a positive integer N_0 such that for all positive integers N divisible by N_0 , we have*

$$(9.11) \quad \mathrm{tr} R(\pi) = |\Delta_f(\pi)| a(G_\pi) O_\pi(\varphi_\pi)$$

Remark 9.5. Using either the results of G. Prasad [23] on the volumes of fundamental domains or the results of Shimura [28] on the exact mass formulas, one can determine the term $a(G_\pi)$ explicitly. The orbital integral $O_\pi(\varphi_\pi)$ is purely local in nature, that is, it is expressed as the product of the local orbital integrals $O_\pi(\varphi_{\pi,v})$. There is also a similar local description as in (9.9). Using this description, it is not hard to show that the local integral $O_\pi(\varphi_{\pi,v})$ is equal to 1 for almost all finite places. We also like to know whether after shrinking the level subgroups U_N at these bad places, each local orbital integral in bad places becomes 1 or becomes easily computable. Nevertheless, we continue to study the global term $|\Delta_f(\pi)|$.

9.5. **A cohomological meaning for $\Delta_f(\pi)$.** Put

$$\Delta(\pi) := \{\gamma \in G(\mathbb{Q}) \mid \gamma \in G(\mathbb{A}) \cdot \pi\} / \sim_{G(\mathbb{Q})}.$$

Lemma 9.6. *We have $\Delta_f(\pi) = \Delta(\pi)$.*

PROOF. Suppose γ is an element in $G(\mathbb{Q})$ which lies in $\Delta_f(\pi)$. It suffices to show that γ is conjugate to π by an element in $G(\mathbb{R})$. Since they are conjugate under $G(\mathbb{Q}_\ell)$, they are conjugate under $G(\overline{\mathbb{Q}}_\ell)$. Therefore, they are $G(\overline{\mathbb{Q}})$ -conjugate and hence $G(\mathbb{C})$ -conjugate. Then the assertion follows from the following lemma.

Lemma 9.7. *Let G be a connected reductive group over \mathbb{R} such that the derived subgroup G_{der} is anisotropic. Then for any two elements x and y in $G(\mathbb{R})$, x and y are $G(\mathbb{R})$ -conjugate if and only if they are $G(\mathbb{C})$ -conjugate.*

PROOF. We first show the case when $G(\mathbb{R})$ is compact. Choose a maximal torus T , which is anisotropic, and any element can be $G(\mathbb{R})$ -conjugate to an element in $T(\mathbb{R})$. Two elements in $T(\mathbb{R})$ are conjugate if and only if they are in the same W_T -orbit, where W_T is the Weyl group of T . Two elements in $T(\mathbb{R})$ are $G(\mathbb{C})$ -conjugate if and only if they are in the same $W_{T_{\mathbb{C}}}$ -orbit, where $W_{T_{\mathbb{C}}}$ is the Weyl group of $T_{\mathbb{C}}$. We have $W_T \simeq W_{T_{\mathbb{C}}}$ and the inclusion $T(\mathbb{R})/W_T \hookrightarrow T(\mathbb{C})/W_{T_{\mathbb{C}}}$. The statement follows.

We reduce to the above special case. Let Z be the connected center of G . Let $S \subset Z$ (resp. $T \subset Z$) be the maximal split (resp. anisotropic) torus. Put $M := G_{\text{der}} \cdot T \cdot S[2]$. One has $G = SM = SM^0$ and the subgroup $M(\mathbb{R})$ meets every component of $G(\mathbb{R})$. We also have $G(\mathbb{R}) = M(\mathbb{R}) \times S(\mathbb{R})^0$; write $x = (x_M, x_S)$ into the M -component and S -component of x . Then two elements x and y are $G(\mathbb{C})$ -conjugate if and only if $x_S = y_S$ and x_M and y_M are $M(\mathbb{C})$ -conjugate. The condition x and y are $M(\mathbb{C})$ -conjugate implies that x and y are in the same component of $M(\mathbb{R})$. Multiplying them an element in $S[2]$, we may assume that x and y are in the connected component $M^0(\mathbb{R})$. Since M^0 is connected and anisotropic, we are done. ■

Proposition 9.8. *We have a natural bijection*

$$(9.12) \quad \Delta(\pi) \simeq \ker [\ker^1(\mathbb{Q}, G_\pi) \rightarrow H^1(\mathbb{Q}, G)],$$

where $\ker^1(\mathbb{Q}, G_\pi)$ is the kernel of the local-global map

$$H^1(\mathbb{Q}, G_\pi) \rightarrow \prod_v H^1(\mathbb{Q}_v, G_\pi)$$

of pointed sets.

PROOF. Let π_1 be an element of $G(\mathbb{Q})$ which lies in $\Delta(\pi)$; the element π_1 is $G(\overline{\mathbb{Q}})$ -conjugate to π . There is an element $g \in G(\overline{\mathbb{Q}})$ such that $g\pi g^{-1} = \pi_1$. For any element $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have

$$\sigma(g)\pi\sigma(g)^{-1} = \pi_1 = g\pi g^{-1}.$$

The map $\sigma \mapsto g^{-1}\sigma(g) \in G_\pi(\overline{\mathbb{Q}})$ is a 1-cycle and defines an element $c \in H^1(\mathbb{Q}, G_\pi)$ whose image in $H^1(\mathbb{Q}, G)$ is the base point. This gives rise to a bijection between the set of $G(\mathbb{Q})$ -conjugacy classes of elements which are $G(\overline{\mathbb{Q}})$ -conjugate to the element π and the set $\ker[H^1(\mathbb{Q}, G_\pi) \rightarrow H^1(\mathbb{Q}, G)]$. The condition that π_1 and π are $G(\mathbb{Q}_v)$ -conjugate imposes the condition that the image c_v of c in $H^1(\mathbb{Q}_v, G_\pi)$ is the base point for all places v . Therefore, the proposition is proved. ■

9.6. Application to the superspecial locus. Let $G, \pi_0 \in G(\mathbb{Q}), U_N$ and $R(\pi_0)$ be those in Section 7, also see Theorem 7.5. In the remaining of this section, We apply the results in this Section to compute the trace $\text{tr } R(\pi_0)$ of the Hecke operator $R(\pi_0)$. Note that this computes the number of \mathbb{F}_p -rational points in $\Lambda_{g,N}^*$ (see Theorem 7.5 (3)). The centralizer G_{π_0} is isomorphic to the group of unitary similitudes of a Hermitian space V over the imaginary quadratic field $\mathbb{Q}(\pi_0) = \mathbb{Q}(\sqrt{-p})$. This group G_{π_0} satisfies the Hasse principle; see a proof below.

Lemma 9.9. *Let E be an imaginary quadratic field and $G = GU(V, \psi)$ be the group of unitary similitudes of a Hermitian space V over E . Then G satisfies the Hasse principle.*

PROOF. This is certainly known to the experts. As we could not find a reference, we provide a proof at the reader's convenience. Note that this is not covered by well-known results of Kottwitz in [16, Section 7]; the group G is of type A but the number $n = \dim_E V$ of variables may not be even.

Consider the short exact sequence

$$1 \longrightarrow G_{\text{der}} \xrightarrow{i} G \xrightarrow{\det} E^\times \longrightarrow 1.$$

This induces the commutative diagram:

$$\begin{array}{ccccccc} E^\times & \longrightarrow & H^1(\mathbb{Q}, G_{\text{der}}) & \longrightarrow & H^1(\mathbb{Q}, G) & \longrightarrow & H^1(\mathbb{Q}, E^\times) = 1 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \prod_v E_v^\times & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, G_{\text{der}}) & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, G) & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, E^\times) = 1 \end{array}$$

The vanishing results

$$H^1(\mathbb{Q}, E^\times) = 1, \quad \text{and} \quad H^1(\mathbb{Q}_v, E^\times) = 1$$

follow from the Shapiro lemma and Hilbert's 90 theorem. By Kneser's theorem one has $H^1(\mathbb{Q}_v, G_{\text{der}}) = 1$ for any finite place v as G_{der} is semi-simple and simply-connected. It follows that $H^1(\mathbb{Q}_v, G) = 1$ for any finite place v . Therefore, we get the commutative diagram:

$$\begin{array}{ccccccc} E^\times & \longrightarrow & H^1(\mathbb{Q}, G_{\text{der}}) & \xrightarrow{i} & H^1(\mathbb{Q}, G) & \longrightarrow & 1 \\ \downarrow & & \downarrow r_\infty^{\text{der}} & & \downarrow r_\infty & & \\ \mathbb{C}^\times & \longrightarrow & H^1(\mathbb{R}, G_{\text{der}}) & \xrightarrow{i_\infty} & H^1(\mathbb{R}, G) & \longrightarrow & 1 \end{array}$$

Since $\det G(\mathbb{R})$ is an open subgroup of \mathbb{C}^\times , which must be \mathbb{C}^\times , the map i_∞ is bijective. Suppose x is an element in $H^1(\mathbb{Q}, G)$ such that $r_\infty(x) = 1$. Choose an element $x' \in H^1(\mathbb{Q}, G_{\text{der}})$ such that $i(x') = x$. Then $r_\infty^{\text{der}}(x') = 1$ as i_∞ is bijective. Since r_∞^{der} is bijective (see [24, Proposition 6.17, p. 284]), $x' = 1$ and it follows that $x = 1$. This proves the lemma. ■

It follows from Lemma 9.6, Proposition 9.8 and Lemma 9.9 that $|\Delta_f(\pi_0)| = |\Delta(\pi_0)| = 1$. By Theorem 9.4, we have proven the following result.

Theorem 9.10. *Let $G, \pi_0 \in G(\mathbb{Q}), U_N$ and $R(\pi_0)$ be as in Section 7. There is a positive integer N_0 such that for all positive integers N divisible by N_0 , we have (see (9.1))*

$$(9.13) \quad \text{tr } R(\pi_0) = a(G_{\pi_0}) O_{\pi_0}(\varphi_{\pi_0}),$$

where the Haar measure on $G_{\pi_0}(\mathbb{A}_f)$ is defined by (9.7).

We also obtain the similar result for the non-principal genus case as treated in Section 8.

ACKNOWLEDGMENTS

The author thanks Professors Ibukiyama and Katsura for their inspiring work [10], especially Ibukiyama for his interest and discussions. He thanks Jiu-Kang Yu and Wen-Wei Li for helpful discussions. The manuscript was prepared during the author's stay at l'Institut des Hautes Études Scientifiques. He acknowledges the institution for kind hospitality and excellent working conditions. The author was partially supported by grants NSC 100-2628-M-001-006-MY4 and AS-99-CDA-M01.

REFERENCES

- [1] M. Borovoi, *Abelian Galois cohomology of reductive groups*. Mem. Amer. Math. Soc. **132** (1998), no. 626, 50 pp.
- [2] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hamburg* **14** (1941), 197–272.
- [3] M. Deuring, Die Anzahl der Typen von Maximalordnungen einer definiten Quaternionenalgebra mit primem Grundzahl. *Jber. Deutsch. Math.* **54** (1950). 24–41.
- [4] T. Ekedahl, On supersingular curves and supersingular abelian varieties. *Math. Scand.* **60** (1987), 151–178.
- [5] L. Fargues, Cohomologie des espaces de modules de groupes p -divisibles et correspondances de Langlands locales. *Astérisques* **291** (2004), 1–199.
- [6] S. Gelbart, *Automorphic forms on adele groups*. Annals of Mathematics Studies, No. 83. Princeton University Press, 1975.
- [7] A. Ghitza, Hecke eigenvalues of Siegel modular forms (mod p) and of algebraic modular forms. *J. Number Theory* **106** (2004), no. 2, 345–384.
- [8] B. H. Gross, Algebraic modular forms. *Israel J. Math.* **113** (1999), 61–93.
- [9] K. Hashimoto and T. Ibukiyama, On class numbers of positive definite binary quaternion hermitian forms, *J. Fac. Sci. Univ. Tokyo* **27** (1980), 549–601.
- [10] T. Ibukiyama and T. Katsura, On the field of definition of superspecial polarized abelian varieties and type numbers. *Compositio Math.* **91** (1994), 37–46.
- [11] T. Ibukiyama, T. Katsura and F. Oort, Supersingular curves of genus two and class numbers. *Compositio Math.* **57** (1986), 127–152.
- [12] T. Katsura and F. Oort, Families of supersingular abelian surfaces, *Compositio Math.* **62** (1987), 107–167.
- [13] R. E. Kottwitz, Rational conjugacy classes in reductive groups. *Duke Math. J.* **49** (1982), no. 4, 785–806.
- [14] R. E. Kottwitz, Stable trace formula: cuspidal tempered terms. *Duke Math. J.* **51** (1984), no. 3, 611–650.
- [15] R. E. Kottwitz, Stable trace formula: elliptic singular terms. *Math. Ann.* **275** (1986), 365–399.
- [16] R. E. Kottwitz, Points on some Shimura varieties over finite fields. *J. Amer. Math. Soc.* **5** (1992), 373–444.
- [17] R.E. Kottwitz, Harmonic analysis on reductive p -adic groups and Lie algebras. *Harmonic analysis, the trace formula, and Shimura varieties*, 393–522, Clay Math. Proc. 4, Amer. Math. Soc., Providence, RI, 2005.
- [18] S. Lang, *Algebraic number theory*. Graduate Texts in Mathematics, **110**. Springer-Verlag, New York, 1986. 354 pp.
- [19] K.-Z. Li and F. Oort, *Moduli of Supersingular Abelian Varieties*. Lecture Notes in Math., vol. 1680, Springer-Verlag, 1998.
- [20] E. Mantovan, On certain unitary group Shimura varieties. *Astérisques* **291** (2004), 201–331.
- [21] D. Mumford, *Abelian Varieties*. Oxford University Press, 1974.

- [22] F. Oort, A stratification of a moduli space of abelian varieties. *Moduli of Abelian Varieties*, 345–416. (ed. by C. Faber, G. van der Geer and F. Oort), Progress in Mathematics **195**, Birkhäuser 2001.
- [23] G. Prasad, Volumes of S -arithmetic quotients of semi-simple groups. *Inst. Hautes Études Sci. Publ. Math.* **69** (1989), 91–117.
- [24] V. Platonov and A. Rapinchuk, Algebraic groups and number theory. *Pure and Applied Mathematics*, 139. Academic Press, Inc., Boston, MA, 1994.
- [25] M. Rapoport and Th. Zink, *Period Spaces for p -divisible groups*. Ann. Math. Studies 141, Princeton Univ. Press, 1996.
- [26] D. A. Reduzzi, Hecke Eigensystems for $(\bmod p)$ Modular Forms of PEL-type and Algebraic Modular Forms, arXiv:1101.3143, 46 pp. To appear in *Int. Math. Res. Not.*
- [27] J.-P. Serre, Two letters on quaternions and modular forms $(\bmod p)$. *Israel J. Math.* **95** (1996), 281–299.
- [28] G. Shimura, *Euler product and Eisenstein series*. CBMS Regional Conference Series in Math., 93, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1997.
- [29] G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*. Publ. Math. Soc. Japan 6, Tokyo, 1961.
- [30] J. Tate, Classes d’isogenie de variétés abéliennes sur un corps fini (d’après T. Honda). *Sém. Bourbaki Exp.* 352 (1968/69). Lecture Notes in Math., vol. 179, Springer-Verlag, 1971.
- [31] E. Viehmann and T. Wedhorn, Ekedahl-Oort and Newton strata for Shimura varieties of PEL type. arXiv:1011.3230, 52 pp.
- [32] A. Weil, The field of definition of a variety. *Amer. J. Math.* **78** (1956), 509–524.
- [33] C.-F. Yu, On the supersingular locus in Hilbert-Blumenthal 4-folds. *J. Algebraic Geom.* **12** (2003), 653–698.
- [34] C.-F. Yu, On reduction of Hilbert-Blumenthal varieties. *Ann. Inst. Fourier (Grenoble)* **53** (2003), 2105–2154.
- [35] C.-F. Yu, On the slope stratification of certain Shimura varieties. *Math. Z.* **251** (2005), 859–873.
- [36] C.-F. Yu, The supersingular loci and mass formulas on Siegel modular varieties. *Doc. Math.* **11** (2006), 449–468.
- [37] C.-F. Yu, Simple mass formulas on Shimura varieties of PEL-type. *Forum Math.* **22** (2010), no. 3, 565–582.
- [38] C.-F. Yu, On the existence of maximal orders. *Int. J. Number Theory* **7** (2011), no. 8, 2091–2114.

INSTITUTE OF MATHEMATICS, ACADEMIA SINICA,, 6TH FLOOR, ASTRONOMY MATHEMATICS BUILDING, NO. 1, ROOSEVELT RD. SEC. 4, TAIPEI, TAIWAN, 10617, AND NCTS (TAIPEI OFFICE)

E-mail address: chiafu@math.sinica.edu.tw